Teoria di Galois e sue applicazioni crittografiche

Parte I: Fondamenti Matematici della Teoria di Galois

Introduzione Storica e Filosofica

La teoria di Galois rappresenta uno dei vertici più straordinari della matematica pura, un capolavoro di astrazione e di potenza concettuale che ha rivoluzionato la nostra comprensione delle equazioni algebriche e delle simmetrie matematiche. Questa teoria, sviluppata dal matematico francese Évariste Galois nei primi decenni del diciannovesimo secolo, costituisce il ponte definitivo tra due mondi apparentemente distanti: la teoria delle equazioni polinomiali e la teoria dei gruppi.

Évariste Galois visse una vita tragicamente breve, morendo in un duello all'età di soli vent'anni nel 1832. Nella notte precedente al duello, consapevole della propria imminente fine, Galois scrisse freneticamente le sue idee matematiche in una lettera indirizzata al suo amico Auguste Chevalier. Quelle pagine contenevano i germi di una teoria che avrebbe cambiato per sempre il corso della matematica, anche se ci vollero decenni prima che la comunità matematica comprendesse appieno la portata rivoluzionaria del suo lavoro.

Il problema fondamentale che Galois si pose era antico quanto la matematica stessa: per quali equazioni polinomiali esiste una formula risolutiva che esprima le soluzioni mediante radicali? L'umanità conosceva da millenni la formula risolutiva per le equazioni di secondo grado, fin dai tempi dei matematici babilonesi. Nel Rinascimento italiano, matematici come Scipione del Ferro, Niccolò Tartaglia e Gerolamo Cardano avevano scoperto le formule per le equazioni di terzo e quarto grado, formule complesse ma pur sempre esprimibili mediante radicali. Ma per le equazioni di quinto grado e superiori, tutti i tentativi erano falliti.

La geniale intuizione di Galois fu di comprendere che la questione della risolubilità mediante radicali non dipende tanto dalla forma dell'equazione quanto dalle simmetrie intrinseche delle sue soluzioni. Egli sviluppò un apparato teorico che associa a ogni equazione polinomiale un oggetto algebrico chiamato gruppo di Galois, il quale codifica tutte le permutazioni delle radici che preservano le relazioni algebriche tra di esse. La risolubilità dell'equazione mediante radicali risulta essere equivalente a una proprietà strutturale di questo gruppo, chiamata risolubilità del gruppo.

Oggi, la teoria di Galois si estende ben oltre il problema originale delle equazioni polinomiali. Essa fornisce il linguaggio naturale per studiare le estensioni di campi, le simmetrie algebriche, e trova applicazioni straordinarie in crittografia, teoria dei codici, geometria algebrica, e persino nella fisica teorica. In particolare, l'uso dei campi finiti e delle loro estensioni è fondamentale nella crittografia moderna, dai cifrari a blocco come l'AES agli algoritmi su curve ellittiche.

Capitolo 1: Richiami di Teoria dei Campi

Prima di addentrarci nel cuore della teoria di Galois, è necessario stabilire solidamente le fondamenta algebriche su cui questa teoria poggia. La teoria dei campi fornisce il linguaggio e gli strumenti essenziali per comprendere le costruzioni galoisiane.

1.1 Definizione e Proprietà Fondamentali dei Campi

Un campo è una delle strutture algebriche più fondamentali in matematica. Intuitivamente, un campo è un insieme in cui possiamo eseguire le quattro operazioni aritmetiche elementari (addizione, sottrazione, moltiplicazione e divisione, quest'ultima esclusa la divisione per zero) e in cui valgono le usuali proprietà associative, commutative e distributive.

Definizione formale: Un campo è una terna $(K, +, \cdot)$ dove K è un insieme non vuoto e $+, \cdot$ sono due operazioni binarie su K, chiamate rispettivamente addizione e moltiplicazione, che soddisfano i seguenti assiomi:

1. **$(K, +)$ è un gruppo abeliano**:
    - Chiusura: Per ogni $a, b \in K$, si ha $a + b \in K$
    - Associatività: Per ogni $a, b, c \in K$, si ha $(a + b) + c = a + (b + c)$
    - Elemento neutro: Esiste un elemento $0 \in K$ tale che $a + 0 = 0 + a = a$ per ogni $a \in K$
    - Elemento inverso: Per ogni $a \in K$ esiste un elemento $-a \in K$ tale che $a + (-a) = (-a) + a = 0$
    - Commutatività: Per ogni $a, b \in K$, si ha $a + b = b + a$
2. **$(K \setminus \{0\}, \cdot)$ è un gruppo abeliano**:
    - Chiusura: Per ogni $a, b \in K \setminus \{0\}$, si ha $a \cdot b \in K \setminus \{0\}$
    - Associatività: Per ogni $a, b, c \in K$, si ha $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
    - Elemento neutro: Esiste un elemento $1 \in K$ con $1 \neq 0$ tale che $a \cdot 1 = 1 \cdot a = a$ per ogni $a \in K$
    - Elemento inverso: Per ogni $a \in K \setminus \{0\}$ esiste un elemento $a^{(-1)} \in K$ tale che $a \cdot a^{(-1)} = a^{(-1)} \cdot a = 1$
    - Commutatività: Per ogni $a, b \in K$, si ha $a \cdot b = b \cdot a$
3. **Proprietà distributiva**: Per ogni $a, b, c \in K$, si ha:
    - $a \cdot (b + c) = a \cdot b + a \cdot c$
    - $(a + b) \cdot c = a \cdot c + b \cdot c$

Questa definizione, apparentemente astratta, cattura l'essenza delle proprietà che ci permettono di "fare aritmetica" in modo coerente. È importante notare che la richiesta di commutatività della moltiplicazione distingue i campi dagli anelli con divisione (detti anche corpi), strutture più generali in cui la moltiplicazione non è necessariamente commutativa.

Esempi fondamentali di campi:

1. **Il campo dei numeri razionali Q**: Questo è forse l'esempio più naturale di campo, costituito da tutte le frazioni a/b dove a, b sono numeri interi e b ≠ 0. L'addizione e la moltiplicazione sono definite nel modo usuale. I numeri razionali hanno la proprietà notevole di essere il più piccolo campo che contiene gli interi Z.

2. **Il campo dei numeri reali R**: Questo campo si ottiene completando Q rispetto alla topologia indotta dal valore assoluto. Geometricamente, R corrisponde alla retta dei numeri reali. La completezza di R significa che ogni successione di Cauchy in R converge a un elemento di R.

3. **Il campo dei numeri complessi C**: Definito come C = {a + bi : a, b ∈ R} dove i è l'unità immaginaria che soddisfa $i^2 = -1$. Questo campo è algebricamente chiuso, il che significa che ogni polinomio non costante a coefficienti in C ha almeno una radice in C. Questa proprietà, nota come teorema fondamentale dell'algebra, è di importanza cruciale.

4. **I campi finiti F_p**: Per ogni numero primo p, l'insieme Z/pZ = {0, 1, 2, ..., p−1} con le operazioni di addizione e moltiplicazione modulo p è un campo. Questi campi finiti sono di importanza fondamentale nella teoria di Galois e nelle applicazioni crittografiche. Ad esempio, F_2 = {0, 1} è il campo più piccolo possibile e gioca un ruolo centrale nella teoria dell'informazione e nella crittografia.

5. **Il campo delle funzioni razionali**: Dato un campo K, possiamo costruire il campo K(x) delle funzioni razionali in una variabile x a coefficienti in K. Gli elementi di K(x) sono espressioni della forma p(x)/q(x) dove p(x) e q(x) sono polinomi in K[x] con q(x) ≠ 0. Questo campo è l'analogo "funzionale" del campo delle frazioni Q rispetto agli interi Z.

1.2 Sottocampi ed Estensioni di Campi

Il concetto di estensione di campi è assolutamente centrale nella teoria di Galois. Intuitivamente, un'estensione di campi è un processo di "ampliamento" di un campo mediante l'aggiunta di nuovi elementi che soddisfano determinate proprietà algebriche.

Definizione: Siano K e L due campi. Diciamo che L è un'estensione di K, e scriviamo K ⊆ L oppure L/K, se K è un sottocampo di L, cioè se K è un sottoinsieme di L che è esso stesso un campo rispetto alle operazioni di L ristrette a K.

Questa relazione di estensione è transitiva: se K ⊆ L e L ⊆ M, allora K ⊆ M. Possiamo quindi costruire torri di estensioni di campi, un concetto che si rivelerà fondamentale.

La struttura di spazio vettoriale: Una delle osservazioni più profonde è che ogni estensione L/K ha una struttura naturale di spazio vettoriale su K. Gli elementi di L sono i vettori, le operazioni di addizione in L definiscono l'addizione vettoriale, e la moltiplicazione di un elemento di L per un elemento di K (vista come scalare) definisce la moltiplicazione per scalare.

Definizione del grado di un'estensione: Il grado dell'estensione L/K, denotato con [L:K], è la dimensione di L come spazio vettoriale su K. Formalmente:

[L:K] = dim_K(L)

Se questa dimensione è finita, diciamo che L/K è un'estensione finita, altrimenti diciamo che è un'estensione infinita.

Teorema della torre (Formula moltiplicativa dei gradi): Siano K ⊆ L ⊆ M estensioni di campi. Allora:

[M:K] = [M:L] · [L:K]

Dimostrazione completa: Supponiamo che [L:K] = m e [M:L] = n siano entrambi finiti. Sia {α_1, α_2, ..., α_m} una base di L su K, e sia {β_1, β_2, ..., β_n} una base di M su L.

Affermiamo che l'insieme B = {α_i · β_j : 1 ≤ i ≤ m, 1 ≤ j ≤ n} è una base di M su K. Questo insieme ha cardinalità mn, il che dimostrerà il teorema.

Dimostrazione che B genera M su K: Sia γ ∈ M un elemento arbitrario. Poiché {β_1, ..., β_n} è una base di M su L, esistono elementi c_1, ..., c_n ∈ L tali che:

γ = c_1 β_1 + c_2 β_2 + ... + c_n β_n

Ora, ogni c_j ∈ L può essere scritto in termini della base {α_1, ..., α_m} di L su K:

c_j = a_(j,1) α_1 + a_(j,2) α_2 + ... + a_(j,m) α_m

dove a_(j,i) ∈ K. Sostituendo, otteniamo:

γ = Σ_(j=1)^n (Σ_(i=1)^m a_(j,i) α_i) β_j = Σ_(i=1)^m Σ_(j=1)^n a_(j,i) (α_i β_j)

Quindi γ è combinazione lineare a coefficienti in K degli elementi di B.

Dimostrazione dell'indipendenza lineare di B su K: Supponiamo che esista una combinazione lineare nulla:

Σ_(i=1)^m Σ_(j=1)^n b_(i,j) α_i β_j = 0

dove b_(i,j) ∈ K. Riorganizzando:

Σ_(j=1)^n (Σ_(i=1)^m b_(i,j) α_i) β_j = 0

Poiché {β_1, ..., β_n} è linearmente indipendente su L, ogni coefficiente deve essere zero:

Σ_(i=1)^m b_(i,j) α_i = 0 per ogni j

Ma poiché {α_1, ..., α_m} è linearmente indipendente su K, questo implica b_(i,j) = 0 per ogni i e j.

Quindi B è effettivamente una base di M su K, e [M:K] = mn = [M:L] · [L:K]. ∎

Questo teorema è di importanza fondamentale perché ci permette di calcolare i gradi di estensioni complesse decomponendole in estensioni più semplici.

1.3 Estensioni Semplici e Elementi Primitivi

Un tipo particolarmente importante di estensione è quello ottenuto aggiungendo un singolo elemento a un campo base.

Definizione: Sia K un campo e α un elemento in qualche estensione di K. L'estensione semplice generata da α, denotata K(α), è il più piccolo campo contenente sia K che α. Formalmente:

$K(\alpha) = \cap \{L : K \subseteq L, \alpha \in L, L \text{ è un campo}\}$

In altre parole, K(α) è l'intersezione di tutti i campi che contengono K e α.

Costruzione esplicita di K(α): Possiamo caratterizzare K(α) in modo più costruttivo. Gli elementi di K(α) sono esattamente tutte le espressioni razionali in α con coefficienti in K. Più precisamente:

$K(\alpha) = \{f(\alpha)/g(\alpha) : f(x), g(x) \in K[x], g(\alpha) \neq 0\}$

dove K[x] denota l'anello dei polinomi in una variabile x a coefficienti in K.

Dobbiamo distinguere due casi fondamentalmente diversi a seconda che α sia algebrico o trascendente su K.

Definizione: Un elemento α in un'estensione di K è detto algebrico su K se esiste un polinomio non nullo $p(x) \in K[x]$ tale che $p(\alpha) = 0$. Altrimenti, α è detto trascendente su K.

Esempio: Il numero $\sqrt{2}$ è algebrico su Q perché soddisfa l'equazione $x^2 - 2 = 0$. Anche $i = \sqrt{(-1)}$ è algebrico su R perché soddisfa $x^2 + 1 = 0$. Per contro, i numeri π ed e sono trascendenti su Q, anche se le dimostrazioni di questi fatti sono profonde e non banali (π fu dimostrato trascendente da Lindemann nel 1882, e da Hermite nel 1873).

Il polinomio minimo: Se α è algebrico su K, tra tutti i polinomi in K[x] che hanno α come radice esiste un unico polinomio monico di grado minimo. Questo polinomio è chiamato polinomio minimo di α su K.

Proposizione: Il polinomio minimo m(x) di α su K ha le seguenti proprietà fondamentali:

1. m(x) è irriducibile in K[x] (cioè non può essere fattorizzato in prodotto di polinomi di grado inferiore in K[x])
2. m(x) divide ogni polinomio $p(x) \in K[x]$ tale che $p(\alpha) = 0$
3. m(x) è unico

Dimostrazione:

(1) Supponiamo per assurdo che $m(x) = a(x) \cdot b(x)$ dove $a(x), b(x) \in K[x]$ hanno grado strettamente minore di deg(m). Allora:

$0 = m(\alpha) = a(\alpha) \cdot b(\alpha)$

Poiché siamo in un campo (e quindi in un dominio di integrità), uno dei due fattori deve essere zero. Ma questo contraddirebbe la minimalità di deg(m).

(2) Sia $p(x) \in K[x]$ tale che $p(\alpha) = 0$. Per l'algoritmo di divisione euclidea in K[x], possiamo scrivere:

$p(x) = q(x) \cdot m(x) + r(x)$

dove $\deg(r) < \deg(m)$. Valutando in α:

$0 = p(\alpha) = q(\alpha) \cdot m(\alpha) + r(\alpha) = 0 + r(\alpha) = r(\alpha)$

Quindi r(x) è un polinomio di grado inferiore a m(x) che si annulla in α. Per la minimalità di deg(m), deve essere r(x) = 0, quindi m(x) divide p(x).

(3) L'unicità segue dal fatto che se m_1(x) e m_2(x) sono entrambi polinomi minimi monici di α, allora m_1 divide m_2 e m_2 divide m_1, quindi m_1 = m_2 (a meno di una costante moltiplicativa, che deve essere 1 dato che entrambi sono monici). ∎

Teorema fondamentale sulle estensioni semplici algebriche: Se α è algebrico su K con polinomio minimo m(x) di grado n, allora:

1. $[K(\alpha):K] = n = \deg(m)$
2. $\{1, \alpha, \alpha^2, ..., \alpha^{(n-1)}\}$ è una base di K(α) su K
3. $K(\alpha) \cong K[x]/(m(x))$ come K-algebre

dove K[x]/(m(x)) denota l'anello quoziente di K[x] modulo l'ideale generato da m(x).

Dimostrazione dettagliata:

(2) Dobbiamo mostrare che $\{1, \alpha, \alpha^2, ..., \alpha^{(n-1)}\}$ è una base di K(α) su K.

Generazione: Ogni elemento di K(α) può essere scritto come $f(\alpha)/g(\alpha)$ dove $f, g \in K[x]$ con $g(\alpha) \neq 0$. Poiché m(x) è il polinomio minimo di α e $\gcd(g(x), m(x)) = 1$ (altrimenti $g(\alpha) = 0$), per il teorema di Bézout esistono polinomi $a(x), b(x) \in K[x]$ tali che:

$a(x) \cdot g(x) + b(x) \cdot m(x) = 1$

Valutando in α:

$a(\alpha) \cdot g(\alpha) = 1$

quindi g(α) è invertibile in K(α) con inverso a(α). Pertanto:

$f(\alpha)/g(\alpha) = f(\alpha) \cdot a(\alpha) \in K[\alpha]$

Ora, usando la divisione euclidea, possiamo scrivere $f(x) \cdot a(x) = q(x) \cdot m(x) + r(x)$ dove $\deg(r) < n$. Quindi:

$f(\alpha) \cdot a(\alpha) = r(\alpha) = c_0 + c_1 \alpha + ... + c_{n-1} \alpha^{n-1}$

per opportuni $c_i \in K$. Quindi $\{1, \alpha, ..., \alpha^{n-1}\}$ genera $K(\alpha)$ su K.

Indipendenza lineare: Supponiamo che:

$c_0 + c_1 \alpha + ... + c_{n-1} \alpha^{n-1} = 0$

dove $c_i \in K$. Allora il polinomio $p(x) = c_0 + c_1 x + ... + c_{n-1} x^{n-1} \in K[x]$ ha grado $< n$ e soddisfa $p(\alpha) = 0$. Poiché $m(x)$ è il polinomio di grado minimo con questa proprietà, deve essere $p(x) = 0$, cioè $c_0 = c_1 = ... = c_{n-1} = 0$.

(1) Segue immediatamente da (2): la dimensione di $K(\alpha)$ su K è n.

(3) Definiamo l'omomorfismo di valutazione $\varphi: K[x] \to K(\alpha)$ mediante $\varphi(p(x)) = p(\alpha)$. Questo è chiaramente un omomorfismo suriettivo di K-algebre. Il nucleo di φ è:

$\ker(\varphi) = \{p(x) \in K[x] : p(\alpha) = 0\}$

Ma abbiamo dimostrato che questo è esattamente l'ideale $(m(x))$ generato da $m(x)$. Per il primo teorema di isomorfismo:

$K[x]/(m(x)) \cong K(\alpha)$

∎

Questo teorema ha conseguenze profonde. Ci dice che studiare un'estensione semplice algebrica equivale a studiare un anello quoziente $K[x]/(m(x))$, dove $m(x)$ è un polinomio irriducibile. Questo punto di vista algebrico sarà fondamentale nello sviluppo della teoria di Galois.

1.4 Chiusura Algebrica e Campi Algebricamente Chiusi

Un concetto di fondamentale importanza è quello di campo algebricamente chiuso.

Definizione: Un campo K è detto algebricamente chiuso se ogni polinomio non costante $p(x) \in K[x]$ ha almeno una radice in K. Equivalentemente, ogni polinomio in $K[x]$ si fattorizza completamente in fattori lineari.

Teorema fondamentale dell'algebra: Il campo $\mathbb{C}$ dei numeri complessi è algebricamente chiuso.

Questo teorema, nonostante il nome, richiede metodi di analisi per la sua dimostrazione. Esistono diverse dimostrazioni, alcune delle quali usano la teoria delle funzioni olomorfe, altre la topologia algebrica. La dimostrazione più elementare, dovuta a Laplace, usa il teorema del valore intermedio del calcolo differenziale.

Chiusura algebrica: Dato un campo K, una chiusura algebrica di K è un'estensione $\bar{K}$ di K che è algebricamente chiusa e tale che ogni elemento di $\bar{K}$ è algebrico su K.

Teorema di esistenza e unicità della chiusura algebrica: Ogni campo K ha una chiusura algebrica $\bar{K}$, e questa è unica a meno di K-isomorfismo.

L'esistenza richiede l'assioma della scelta o un principio equivalente (come il lemma di Zorn). L'unicità invece può essere dimostrata costruttivamente.

Esempi fondamentali:

1. La chiusura algebrica di R è C. Infatti, ogni numero complesso è algebrico su R (ogni numero complesso è radice di un polinomio di grado al massimo 2 a coefficienti reali).

2. La chiusura algebrica di Q è il campo $\bar{Q}$ dei numeri algebrici, cioè l'insieme di tutti i numeri complessi che sono radici di qualche polinomio a coefficienti razionali. Il campo $\bar{Q}$ è numerabile (perché possiamo enumerare tutti i polinomi a coefficienti razionali e per ognuno le sue radici), mentre C non è numerabile. Questo dimostra che "quasi tutti" i numeri complessi sono trascendenti su Q.

3. Per un campo finito F_p, la sua chiusura algebrica $\bar{F}_p$ è un'unione numerabile di campi finiti. Più precisamente, $\bar{F}_p$ contiene, per ogni intero positivo n, un unico sottocampo con p^n elementi, e $\bar{F}_p$ è l'unione di tutti questi sottocampi al variare di n.

1.5 Campi di Spezzamento

Un concetto centrale nella teoria di Galois è quello di campo di spezzamento di un polinomio.

Definizione: Sia K un campo e $p(x) \in K[x]$ un polinomio non costante. Un campo di spezzamento (o campo di decomposizione) di p(x) su K è un'estensione L di K tale che:

1. p(x) si fattorizza completamente in fattori lineari in L[x]
2. L è generato su K dalle radici di p(x)

La seconda condizione significa che L è il più piccolo campo contenente K e tutte le radici di p(x). Se $\alpha_1, \alpha_2, ..., \alpha_n$ sono le radici di p(x) in una qualche estensione, allora:

$L = K(\alpha_1, \alpha_2, ..., \alpha_n)$

Teorema di esistenza e unicità: Per ogni campo K e ogni polinomio non costante $p(x) \in K[x]$, esiste un campo di spezzamento di p(x) su K, ed esso è unico a meno di K-isomorfismo.

Dimostrazione dell'esistenza per induzione sul grado:

Sia n = deg(p). Se n = 1, allora p(x) = ax + b è già lineare, quindi K stesso è il campo di spezzamento.

Supponiamo $n > 1$. Sia $m(x)$ un fattore irriducibile di $p(x)$ in $K[x]$. Consideriamo l'estensione $K_1 = K[x]/(m(x))$. Sia α l'immagine di x in K_1. Allora α è una radice di $m(x)$, e quindi anche di $p(x)$.

Possiamo fattorizzare $p(x)$ in $K_1[x]$:

$$p(x) = (x - \alpha) \cdot q(x)$$

dove $q(x) \in K_1[x]$ ha grado $n - 1$. Per ipotesi induttiva, esiste un campo di spezzamento L di $q(x)$ su K_1. Chiaramente L contiene tutte le radici di $p(x)$ (la radice α era già in $K_1 \subseteq L$, e le altre radici sono radici di $q(x)$, quindi stanno in L). Inoltre, L è generato su K dalle radici di $p(x)$, quindi L è un campo di spezzamento di $p(x)$ su K. ∎

Dimostrazione dell'unicità: Siano L e L' due campi di spezzamento di $p(x)$ su K. Dobbiamo costruire un K-isomorfismo $\varphi: L \to L'$.

La dimostrazione procede per induzione su $[L:K]$. Se $[L:K] = 1$, allora $L = K = L'$, e non c'è nulla da dimostrare.

Supponiamo $[L:K] > 1$. Allora $p(x)$ ha un fattore irriducibile $m(x)$ di grado > 1 in $K[x]$. Sia α una radice di $m(x)$ in L. Allora $K(\alpha) \subseteq L$ e $[K(\alpha):K] = \deg(m) > 1$.

Analogamente, in L' esiste una radice α' di $m(x)$. L'isomorfismo $K[x]/(m(x)) \cong K(\alpha)$ e $K[x]/(m(x)) \cong K(\alpha')$ ci fornisce un K-isomorfismo $\sigma: K(\alpha) \to K(\alpha')$ che mappa α in α'.

Ora, L è un campo di spezzamento di $p(x)$ su $K(\alpha)$, e L' è un campo di spezzamento di $\sigma(p(x)) = p(x)$ su $K(\alpha')$. Poiché $[L:K(\alpha)] < [L:K]$, per ipotesi induttiva esiste un $K(\alpha)$-isomorfismo $\tau: L \to L'$ che estende σ. Questo τ è anche un K-isomorfismo, come volevamo. ∎

Esempio fondamentale: Consideriamo $p(x) = x^2 - 2 \in Q[x]$. Le radici di questo polinomio sono $\pm\sqrt{2}$. Il campo di spezzamento è:

$$L = Q(\sqrt{2}, -\sqrt{2}) = Q(\sqrt{2})$$

perché $-\sqrt{2} = -1 \cdot \sqrt{2} \in Q(\sqrt{2})$. Abbiamo $[L:Q] = 2$, con base $\{1, \sqrt{2}\}$.

Esempio più complesso: Consideriamo $p(x) = x^4 - 2 \in Q[x]$. Per trovare le radici, osserviamo che se $\alpha^4 = 2$, allora $(\alpha^2)^2 = 2$, quindi $\alpha^2 = \pm\sqrt[4]{2}$. Le quattro radici sono:

$$\alpha_1 = \sqrt[4]{2} \quad \alpha_2 = i \cdot \sqrt[4]{2}$$
$$\alpha_3 = -\sqrt[4]{2} \quad \alpha_4 = -i \cdot \sqrt[4]{2}$$

dove $\sqrt[4]{2}$ denota la radice reale positiva. Il campo di spezzamento è:

$$L = Q(\sqrt[4]{2}, i)$$

Calcoliamo il grado di questa estensione. Abbiamo la torre:

$$Q \subseteq Q(\sqrt[4]{2}) \subseteq Q(\sqrt[4]{2}, i)$$

Il polinomio minimo di $\sqrt[4]{2}$ su Q è $x^4 - 2$ (si può verificare che è irriducibile usando il criterio di Eisenstein con p = 2). Quindi $[Q(\sqrt[4]{2}):Q] = 4$.

Il polinomio minimo di i su $Q(\sqrt[4]{2})$ è $x^2 + 1$ (che rimane irriducibile perché $Q(\sqrt[4]{2}) \subseteq R$ e $i \notin R$). Quindi $[Q(\sqrt[4]{2}, i):Q(\sqrt[4]{2})] = 2$.

Per la formula della torre:

$[L:Q] = [Q(\sqrt[4]{2}, i):Q(\sqrt[4]{2})] \cdot [Q(\sqrt[4]{2}):Q] = 2 \cdot 4 = 8$

1.6 Estensioni Normali e Separabili

Due proprietà fondamentali delle estensioni di campi sono la normalità e la separabilità. Queste proprietà sono essenziali per caratterizzare le estensioni galoisiane.

Definizione (Estensione normale): Un'estensione finita L/K è detta normale se ogni polinomio irriducibile in K[x] che ha almeno una radice in L si spezza completamente in L[x] (cioè ha tutte le sue radici in L).

Questa condizione può sembrare tecnica, ma ha un significato geometrico profondo: un'estensione normale è "chiusa" rispetto alle operazioni di coniugio algebrico. Se un elemento algebrico α appartiene a L, allora tutti i suoi "coniugati" (le altre radici del suo polinomio minimo) appartengono anch'essi a L.

Teorema di caratterizzazione delle estensioni normali: Sia L/K un'estensione finita. Le seguenti condizioni sono equivalenti:

1. L/K è normale
2. L è il campo di spezzamento di qualche famiglia di polinomi in K[x]
3. L è il campo di spezzamento di un singolo polinomio in K[x]
4. Per ogni K-omomorfismo $\sigma: L \to \bar{K}$ (dove $\bar{K}$ è una chiusura algebrica di K), si ha $\sigma(L) = L$

Dimostrazione:

(1) $\Rightarrow$ (2): Sia L/K normale e finita. Allora $L = K(\alpha_1, ..., \alpha_n)$ per qualche insieme finito di elementi. Sia $m_i(x)$ il polinomio minimo di α_i su K. Per la normalità, ogni $m_i(x)$ si spezza completamente in L. Quindi L è il campo di spezzamento della famiglia $\{m_1(x), ..., m_n(x)\}$.

(2) $\Rightarrow$ (3): Se L è il campo di spezzamento di $\{p_1(x), ..., p_r(x)\}$, allora L è anche il campo di spezzamento del singolo polinomio $p(x) = p_1(x) \cdot p_2(x) \cdot ... \cdot p_r(x)$.

(3) $\Rightarrow$ (1): Sia L il campo di spezzamento di $p(x) \in K[x]$. Sia q(x) un polinomio irriducibile in K[x] che ha una radice β in L. Dobbiamo mostrare che q(x) si spezza completamente in L.

Sia β' un'altra radice di q(x) in $\bar{K}$. Poiché q(x) è il polinomio minimo di entrambi β e β', esiste un K-isomorfismo $\tau: K(\beta) \to K(\beta')$ tale che $\tau(\beta) = \beta'$.

Ora, L è il campo di spezzamento di p(x) su K, e quindi anche su K(β). Analogamente, τ(L) è il campo di spezzamento di p(x) su K(β'). Per l'unicità del campo di spezzamento, esiste un K(β')-isomorfismo che estende τ a un K-isomorfismo σ: L → τ(L).

Ma L contiene tutte le radici di p(x), e σ permuta queste radici. Poiché L è generato da K e dalle radici di p(x), e σ fissa K e permuta le radici, deve essere σ(L) ⊆ L. Poiché σ è iniettivo e L è finito, σ è suriettivo, quindi σ(L) = L.

In particolare, β' = τ(β) = σ(β) ∈ σ(L) = L. Quindi ogni radice di q(x) sta in L.

(3) ⟹ (4): Sia σ: L → $\bar{K}$ un K-omomorfismo. Se L è il campo di spezzamento di p(x) su K, allora σ(L) è il campo di spezzamento di σ(p(x)) = p(x) su K (perché σ fissa K). Ma l'unicità del campo di spezzamento implica che σ(L) ≅_K L, e poiché σ(L) ⊆ $\bar{K}$ contiene L, deve essere σ(L) = L.

(4) ⟹ (1): Sia q(x) irriducibile in K[x] con una radice β ∈ L. Sia β' un'altra radice di q(x) in $\bar{K}$. Come prima, esiste un K-isomorfismo τ: K(β) → K(β') con τ(β) = β'. Questo si estende a un K-omomorfismo σ: L → $\bar{K}$. Per ipotesi, σ(L) = L, quindi β' = τ(β) ∈ τ(K(β)) ⊆ σ(L) = L. ∎

Esempi:

1. Q(√2)/Q è normale: il polinomio minimo di √2 è $x^2 - 2$, che si spezza come $(x - \sqrt{2})(x + \sqrt{2})$ in Q(√2)[x].

2. Q($\sqrt[4]{2}$)/Q NON è normale: il polinomio minimo di $\sqrt[4]{2}$ è $x^4 - 2$, ma questo polinomio ha anche le radici complesse $i \cdot \sqrt[4]{2}$ e $-i \cdot \sqrt[4]{2}$, che non appartengono a Q($\sqrt[4]{2}$) (perché Q($\sqrt[4]{2}$) ⊆ R).

3. Q($\sqrt[4]{2}$, i)/Q è normale: è il campo di spezzamento di $x^4 - 2$.

Definizione (Molteplicità di una radice): Sia p(x) ∈ K[x] e sia α una radice di p(x) in qualche estensione. La molteplicità di α come radice di p(x) è il più grande intero m tale che (x − α)^m divide p(x) in K(α)[x].

Definizione (Polinomio separabile): Un polinomio irriducibile p(x) ∈ K[x] è detto separabile se tutte le sue radici in una chiusura algebrica $\bar{K}$ sono distinte (cioè hanno molteplicità 1). Un polinomio arbitrario è separabile se tutti i suoi fattori irriducibili sono separabili.

Definizione (Estensione separabile): Un'estensione finita L/K è detta separabile se ogni α ∈ L ha polinomio minimo separabile su K. Equivalentemente, se L = K(α_1, ..., α_n) dove ogni α_i è separabile su K.

La separabilità è automatica in molti casi importanti:

Teorema: Ogni estensione di un campo di caratteristica zero è separabile.

Dimostrazione: Sia K un campo di caratteristica zero e p(x) ∈ K[x] irriducibile. Dobbiamo mostrare che p(x) è separabile.

Supponiamo per assurdo che p(x) abbia una radice multipla α in $\bar{K}$. Allora $(x - \alpha)^2$ divide p(x) in $\bar{K}[x]$. Questo significa che α è anche radice della derivata p'(x).

Ma se p(x) è irriducibile di grado $n \geq 1$, allora p'(x) ha grado $n - 1 < n$. Se $p'(x) \neq 0$, allora α essendo radice comune a p(x) e p'(x) implicherebbe che gcd(p(x), p'(x)) è un polinomio non costante che divide p(x), contraddicendo l'irriducibilità di p(x).

Quindi deve essere p'(x) = 0. Ma in un campo di caratteristica zero, la derivata di un polinomio non costante non può essere identicamente nulla (se $p(x) = \Sigma\ a_i\ x^i$ con qualche $a_n \neq 0$ e $n \geq 1$, allora il coefficiente di $x^{(n-1)}$ in p'(x) è $n \cdot a_n \neq 0$ perché $n \neq 0$ in K). Contraddizione. ∎

Teorema: Ogni estensione di un campo finito è separabile.

Questo risultato è meno ovvio ma altrettanto importante. La dimostrazione usa il fatto che il gruppo di automorfismi di un campo finito (il cosiddetto automorfismo di Frobenius) è ciclico.

Nei campi di caratteristica positiva possono esistere estensioni non separabili, dette inseparabili. Ad esempio, se $K = F_p(t)$ è il campo delle funzioni razionali su F_p, e consideriamo α tale che $\alpha^p = t$, allora il polinomio minimo di α su K è $x^p - t$, che ha α come radice di molteplicità p (perché $x^p - t = (x - \alpha)^p$ in $K(\alpha)[x]$, usando il fatto che in caratteristica p il binomio di Newton si semplifica drasticamente).

1.7 Estensioni Galoisiane: La Sintesi

Siamo ora pronti per definire il tipo di estensione che è al centro della teoria di Galois.

Definizione: Un'estensione finita L/K è detta galoisiana (o estensione di Galois) se è sia normale che separabile.

Le estensioni galoisiane sono quelle per cui la teoria di Galois funziona perfettamente, stabilendo una corrispondenza biunivoca tra sottogruppi del gruppo di Galois e campi intermedi.

Esempi fondamentali:

1. Ogni estensione finita di Q è separabile (perché Q ha caratteristica zero), quindi è galoisiana se e solo se è normale. Ad esempio:
    - $Q(\sqrt{2})/Q$ è galoisiana
    - $Q(\sqrt[4]{2})/Q$ non è galoisiana (non normale)
    - $Q(\sqrt[4]{2}, i)/Q$ è galoisiana (campo di spezzamento di $x^4 - 2$)
2. Ogni estensione finita di un campo finito è galoisiana (perché le estensioni di campi finiti sono sempre normali e separabili).

3. L'estensione C/R è galoisiana: C è il campo di spezzamento di $x^2 + 1$ su R, quindi è normale, ed è separabile perché R ha caratteristica zero.

Teorema di caratterizzazione alternativa: Un'estensione finita L/K è galoisiana se e solo se L è il campo di spezzamento di un polinomio separabile in K[x].

Dimostrazione:

(⟹) Se L/K è galoisiana, allora è normale, quindi L è il campo di spezzamento di qualche polinomio p(x) ∈ K[x]. Essendo L/K separabile, possiamo assumere che p(x) sia separabile (eliminando eventuali fattori multipli).

(⟸) Se L è il campo di spezzamento di un polinomio separabile p(x), allora L/K è normale per definizione. Per la separabilità, ogni α ∈ L è una funzione razionale delle radici di p(x), che sono tutte separabili, quindi α è separabile su K. ∎

Capitolo 2: Il Gruppo di Galois

Il concetto centrale della teoria di Galois è il gruppo di Galois, che codifica le simmetrie di un'estensione di campi.

2.1 Automorfismi di Campi

Definizione: Un automorfismo di un campo L è un isomorfismo di campi σ: L → L. L'insieme di tutti gli automorfismi di L, denotato Aut(L), forma un gruppo rispetto alla composizione di funzioni.

Verifichiamo che Aut(L) è effettivamente un gruppo:

- Chiusura: La composizione di due automorfismi è un automorfismo
- Associatività: La composizione di funzioni è associativa
- Identità: L'applicazione identità id: L → L è un automorfismo
- Inversi: Ogni automorfismo ha un inverso (che è ancora un automorfismo)

Definizione: Sia L/K un'estensione di campi. Un K-automorfismo di L è un automorfismo σ: L → L tale che σ(k) = k per ogni k ∈ K (cioè σ fissa K elemento per elemento). L'insieme di tutti i K-automorfismi di L è denotato Aut_K(L) o Aut(L/K).

È facile verificare che Aut(L/K) è un sottogruppo di Aut(L).

Proposizione: Sia L/K un'estensione finita e σ ∈ Aut(L/K). Allora:

1. Se α ∈ L è algebrico su K con polinomio minimo m(x), allora σ(α) è anch'esso una radice di m(x)
2. Se L = K(α), allora σ è completamente determinato dal valore σ(α)

Dimostrazione:

(1) Sia m(x) = a_0 + a_1 x + ... + a_n x^n ∈ K[x] con m(α) = 0. Applicando σ:

0 = σ(0) = σ(m(α)) = σ(a_0 + a_1 α + ... + a_n α^n) = σ(a_0) + σ(a_1) σ(α) + ... + σ(a_n) σ(α)^n = a_0 + a_1 σ(α) + ... + a_n σ(α)^n (perché σ fissa K) = m(σ(α))

Quindi σ(α) è radice di m(x).

(2) Ogni elemento di L = K(α) può essere scritto come p(α)/q(α) dove p, q ∈ K[x] con q(α) ≠ 0. Allora:

σ(p(α)/q(α)) = σ(p(α))/σ(q(α)) = p(σ(α))/q(σ(α))

Quindi σ è completamente determinato da σ(α). ∎

Questo risultato è fondamentale: ci dice che i K-automorfismi di L permutano le radici dei polinomi minimali. Questo giustifica l'interpretazione dei Galois come "gruppo di simmetrie" dell'estensione.

2.2 Definizione del Gruppo di Galois

Definizione: Sia L/K un'estensione di campi (non necessariamente finita). Il gruppo di Galois di L su K, denotato Gal(L/K), è il gruppo di tutti i K-automorfismi di L:

Gal(L/K) = Aut(L/K) = {σ: L → L : σ è isomorfismo, σ(k) = k per ogni k ∈ K}

Esempio fondamentale: Consideriamo l'estensione Q(√2)/Q.

Il campo Q(√2) = {a + b√2 : a, b ∈ Q}. Ogni σ ∈ Gal(Q(√2)/Q) deve soddisfare:

- σ fissa Q
- σ(√2) è una radice di $x^2 - 2$ (il polinomio minimo di √2)

Le uniche radici di $x^2 - 2$ in Q(√2) sono ±√2. Quindi abbiamo due possibilità:

1. σ_1(√2) = √2: questo dà l'automorfismo identità σ_1(a + b√2) = a + b√2

2. σ_2(√2) = −√2: questo dà l'automorfismo σ_2(a + b√2) = a − b√2

Possiamo verificare che σ_2 è effettivamente un automorfismo:

- σ_2((a + b√2) + (c + d√2)) = σ_2((a+c) + (b+d)√2) = (a+c) − (b+d)√2 = σ_2(a + b√2) + σ_2(c + d√2)
- σ_2((a + b√2)(c + d√2)) = σ_2((ac + 2bd) + (ad + bc)√2) = (ac + 2bd) − (ad + bc)√2 = (a − b√2)(c − d√2) = σ_2(a + b√2) · σ_2(c + d√2)

Quindi Gal(Q(√2)/Q) = {σ_1, σ_2} ≅ Z/2Z, il gruppo ciclico di ordine 2.

Esempio più complesso: Consideriamo Q(⁴√2, i)/Q, il campo di spezzamento di $x^4 - 2$.

Le radici di $x^4 - 2$ sono α_1 = ⁴√2, α_2 = i·⁴√2, α_3 = −⁴√2, α_4 = −i·⁴√2.

Ogni σ ∈ Gal(Q(⁴√2, i)/Q) deve permutare queste radici. Inoltre:

- σ è determinato da σ(⁴√2) e σ(i)
- σ(⁴√2) deve essere una radice di $x^4 - 2$

- $\sigma(i)$ deve essere una radice di $x^2 + 1$, quindi $\sigma(i) \in \{i, -i\}$

Enumerando le possibilità:

Se $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$:

- $\sigma(i) = i \Longrightarrow \sigma = id$
- $\sigma(i) = -i \Longrightarrow \sigma = \rho$ (complesso coniugato)

Se $\sigma(\sqrt[4]{2}) = i \cdot \sqrt[4]{2}$:

- $\sigma(i) = i \Longrightarrow \sigma = \tau$ (rotazione)
- $\sigma(i) = -i \Longrightarrow \sigma = \tau\rho$

Se $\sigma(\sqrt[4]{2}) = -\sqrt[4]{2}$:

- $\sigma(i) = i \Longrightarrow \sigma = \tau^2$ (inversione)
- $\sigma(i) = -i \Longrightarrow \sigma = \tau^2\rho$

Se $\sigma(\sqrt[4]{2}) = -i \cdot \sqrt[4]{2}$:

- $\sigma(i) = i \Longrightarrow \sigma = \tau^3$
- $\sigma(i) = -i \Longrightarrow \sigma = \tau^3\rho$

Il gruppo $Gal(Q(\sqrt[4]{2}, i)/Q)$ ha 8 elementi e si può dimostrare che è isomorfo al gruppo diedrale D_4 (il gruppo delle simmetrie di un quadrato).

Struttura esplicita:

- $\rho^2 = id$ (ρ è di ordine 2)
- $\tau^4 = id$ (τ è di ordine 4)
- $\rho\tau = \tau^3\rho$ (relazione di non commutatività)

2.3 Il Teorema Fondamentale: Ordine del Gruppo di Galois

Il risultato centrale che collega il gruppo di Galois al grado dell'estensione è il seguente:

Teorema di Artin: Sia L/K un'estensione finita e sia G = Gal(L/K) il suo gruppo di Galois. Sia L^G = {$\alpha \in L : \sigma(\alpha) = \alpha$ per ogni $\sigma \in G$} il campo fisso di G (cioè il sottocampo di L costituito dagli elementi fissati da tutti gli automorfismi in G). Allora:

1. $K \subseteq L^G$
2. $[L:L^G] = |G|$
3. L/L^G è galoisiana

Corollario immediato: Se L/K è galoisiana, allora $L^G = K$ e $|Gal(L/K)| = [L:K]$.

Questo corollario è il cuore della teoria di Galois per estensioni finite: per un'estensione galoisiana, il gruppo di Galois ha ordine esattamente uguale al grado dell'estensione.

Dimostrazione del Teorema di Artin (schema):

La parte più delicata è dimostrare (2). L'idea è utilizzare l'indipendenza lineare degli automorfismi.

Lemma di Dedekind (Indipendenza lineare degli automorfismi): Sia L un campo e G un insieme di automorfismi distinti di L. Allora gli elementi di G sono linearmente indipendenti come funzioni da L a L (visti come spazio vettoriale su L).

Più precisamente: se $\sigma_1, ..., \sigma_n \in G$ sono distinti e $a_1, ..., a_n \in L$ soddisfano:

$a_1 \sigma_1(x) + a_2 \sigma_2(x) + ... + a_n \sigma_n(x) = 0$ per ogni $x \in L$

allora $a_1 = a_2 = ... = a_n = 0$.

Dimostrazione del lemma: Per induzione su n. Il caso n = 1 è banale (se $a_1 \sigma_1(x) = 0$ per ogni x, prendendo x = 1 otteniamo $a_1 = 0$).

Supponiamo $n > 1$ e che il risultato valga per $n - 1$. Sia:

$a_1 \sigma_1(x) + ... + a_n \sigma_n(x) = 0$ per ogni $x \in L$

Se tutti gli a_i fossero zero, avremmo finito. Supponiamo per assurdo che non siano tutti zero. Possiamo assumere $a_n \neq 0$ (rinumerando se necessario).

Poiché $\sigma_1 \neq \sigma_n$, esiste $y \in L$ tale che $\sigma_1(y) \neq \sigma_n(y)$. Sostituendo xy al posto di x nella relazione:

$a_1 \sigma_1(xy) + ... + a_n \sigma_n(xy) = 0$ $a_1 \sigma_1(x)\sigma_1(y) + ... + a_n \sigma_n(x)\sigma_n(y) = 0$

Moltiplicando la relazione originale per $\sigma_n(y)$:

$a_1 \sigma_1(x)\sigma_n(y) + ... + a_n \sigma_n(x)\sigma_n(y) = 0$

Sottraendo:

$a_1 \sigma_1(x)(\sigma_1(y) - \sigma_n(y)) + ... + a_{(n-1)} \sigma_{(n-1)}(x)(\sigma_{(n-1)}(y) - \sigma_n(y)) = 0$

Questa è una relazione lineare con $n - 1$ automorfismi. Per ipotesi induttiva, tutti i coefficienti sono zero. In particolare:

$a_1(\sigma_1(y) - \sigma_n(y)) = 0$

Ma $\sigma_1(y) - \sigma_n(y) \neq 0$ per scelta di y, quindi $a_1 = 0$. Allo stesso modo, $a_2 = ... = a_{(n-1)} = 0$. Dalla relazione originale, anche $a_n = 0$, contraddicendo la nostra assunzione. ∎

Ora usiamo questo lemma per dimostrare $[L:L^G] = |G|$.

Sia $G = \{\sigma_1, ..., \sigma_n\}$ dove $n = |G|$. Dobbiamo mostrare che $\dim_{(L^G)}(L) = n$.

Prima dimostriamo che $\dim_{(L^G)}(L) \leq n$. Supponiamo per assurdo che esistano $n + 1$ elementi $\alpha_1, ..., \alpha_{(n+1)} \in L$ linearmente indipendenti su L^G. Consideriamo il sistema di n equazioni lineari in $n + 1$ incognite $x_1, ..., x_{(n+1)}$:

$\sigma_i(\alpha_1) x_1 + \sigma_i(\alpha_2) x_2 + ... + \sigma_i(\alpha_{n+1}) x_{n+1} = 0$ per $i = 1, ..., n$

Questo sistema ha più incognite che equazioni, quindi ha una soluzione non banale $(c_1, ..., c_{n+1})$ in L con qualche $c_j \neq 0$. Possiamo assumere che il numero di c_j non nulli sia minimo tra tutte le soluzioni non banali.

Moltiplicando l'i-esima equazione per un coefficiente opportuno e sommando, possiamo assumere $c_{n+1} = 1$ (rinormalizzando). Se qualche $c_j \notin L^G$, diciamo $c_1 \notin L^G$, allora esiste $\sigma_k \in G$ tale che $\sigma_k(c_1) \neq c_1$.

Applicando σ_k a ogni equazione:

$\sigma_k(\sigma_i(\alpha_1)) \sigma_k(c_1) + ... + \sigma_k(\sigma_i(\alpha_{n+1})) \sigma_k(c_{n+1}) = 0$

Ma $\sigma_k(\sigma_i(\alpha_j)) = (\sigma_k \circ \sigma_i)(\alpha_j)$, e poiché G è un gruppo, quando i varia da 1 a n, anche $\sigma_k \circ \sigma_i$ varia su tutto G (in ordine diverso). Quindi otteniamo ancora il sistema originale con coefficienti $\sigma_k(c_j)$.

Sottraendo termine a termine:

$\sigma_i(\alpha_1)(\sigma_k(c_1) - c_1) + ... + \sigma_i(\alpha_n)(\sigma_k(c_n) - c_n) = 0$

Questo è una soluzione con meno coefficienti non nulli (perché $\sigma_k(c_{n+1}) - c_{n+1} = 1 - 1 = 0$), contraddicendo la minimalità. Quindi tutti i $c_j \in L^G$.

Ma allora, per l'indipendenza lineare degli α_j su L^G, tutti i $c_j = 0$, contraddicendo $c_{n+1} = 1$.

Quindi $\dim_{L^G}(L) \leq n$.

Per dimostrare l'uguaglianza, usiamo un argomento di teoria dei campi più avanzato (che omettiamo per brevità). L'idea è che se $\dim_{L^G}(L) < n$, allora il lemma di Dedekind implicherebbe l'esistenza di più automorfismi, contraddicendo $|G| = n$. ∎

Esempi di applicazione:

1. $Gal(Q(\sqrt{2})/Q) = \{id, \sigma\}$ con $|Gal(Q(\sqrt{2})/Q)| = 2 = [Q(\sqrt{2}):Q]$. ✓
2. $Gal(Q(\sqrt[4]{2}, i)/Q) \cong D_4$ con $|Gal(Q(\sqrt[4]{2}, i)/Q)| = 8 = [Q(\sqrt[4]{2}, i):Q]$. ✓
3. Per l'estensione C/R, abbiamo $Gal(C/R) = \{id, conj\}$ dove conj è la coniugazione complessa. $|Gal(C/R)| = 2 = [C:R]$. ✓

Capitolo 3: Il Teorema Fondamentale della Teoria di Galois

Il teorema fondamentale stabilisce una corrispondenza biunivoca tra i sottocampi di un'estensione galoisiana e i sottogruppi del gruppo di Galois.

3.1 Corrispondenza di Galois

Sia L/K un'estensione galoisiana finita con gruppo di Galois G = Gal(L/K).

Definiamo due operazioni:

- Per ogni sottogruppo $H \subseteq G$, definiamo il campo fisso: $L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ per ogni } \sigma \in H\}$
- Per ogni campo intermedio $K \subseteq E \subseteq L$, definiamo il gruppo di stabilità: $Gal(L/E) = \{\sigma \in G : \sigma(e) = e \text{ per ogni } e \in E\}$

Teorema Fondamentale della Teoria di Galois: Sia L/K galoisiana finita con G = Gal(L/K). Allora:

1. Le mappe $H \mapsto L^H$ e $E \mapsto Gal(L/E)$ sono inverse l'una dell'altra, stabilendo una corrispondenza biunivoca tra: {sottogruppi H di G} $\leftrightarrow$ {campi intermedi $K \subseteq E \subseteq L$}

2. Questa corrispondenza inverte l'inclusione: $H_1 \subseteq H_2 \Leftrightarrow L^{(H_2)} \subseteq L^{(H_1)}$

3. Per ogni campo intermedio E:

    - $[L:E] = |Gal(L/E)|$
    - $[E:K] = |G|/|Gal(L/E)| = [G : Gal(L/E)]$
4. L'estensione E/K è normale (e quindi galoisiana) se e solo se Gal(L/E) è un sottogruppo normale di G. In tal caso: $Gal(E/K) \cong G / Gal(L/E)$

Dimostrazione (punti principali):

(1) Dobbiamo dimostrare che:

- $Gal(L/L^H) = H$ per ogni sottogruppo H
- $L^{(Gal(L/E))} = E$ per ogni campo intermedio E

La prima è diretta dal teorema di Artin: $Gal(L/L^H)$ è il gruppo di automorfismi che fissano L^H, che è esattamente H per definizione.

Per la seconda proprietà del Teorema Fondamentale, chiaramente $E \subseteq L^{(Gal(L/E))}$ (perché ogni $\sigma \in Gal(L/E)$ fissa E per definizione). Per l'inclusione opposta, usiamo il fatto che:

$[L:E] = |Gal(L/E)|$ (per il teorema di Artin applicato a L/E)

e

$[L:L^{(Gal(L/E))}] = |Gal(L/E)|$ (ancora per il teorema di Artin)

Quindi $[L:E] = [L:L^{(Gal(L/E))}]$. Poiché $E \subseteq L^{(Gal(L/E))}$, questo implica $E = L^{(Gal(L/E))}$.

(2) L'inversione delle inclusioni segue direttamente dalle definizioni: se $H_1 \subseteq H_2$, allora ci sono più automorfismi in H_2 che fissano elementi, quindi $L^{(H_2)} \subseteq L^{(H_1)}$.

(3) Abbiamo già dimostrato [L:E] = |Gal(L/E)|. Per la seconda formula, usiamo la formula della torre:

[L:K] = [L:E] · [E:K]

Quindi:

[E:K] = [L:K]/[L:E] = |G|/|Gal(L/E)| = [G : Gal(L/E)]

dove [G : Gal(L/E)] denota l'indice del sottogruppo Gal(L/E) in G.

(4) Questa è la parte più profonda. Dimostriamo entrambe le direzioni.

(⟹) Supponiamo E/K normale. Dobbiamo mostrare che Gal(L/E) è normale in G.

Sia σ ∈ G e τ ∈ Gal(L/E). Dobbiamo mostrare che σ τ σ^(−1) ∈ Gal(L/E), cioè che σ τ σ^(−1) fissa E.

Sia e ∈ E. Poiché E/K è normale, e σ è un K-automorfismo di L, la restrizione di σ a E mappa E in E (questo è il contenuto della normalità: ogni K-omomorfismo mappa E in E). Quindi σ(e) ∈ E.

Ora:

(σ τ σ^(−1))(e) = σ(τ(σ^(−1)(e)))

Poiché σ mappa E in E, abbiamo σ^(−1)(e) ∈ E. Poiché τ ∈ Gal(L/E), abbiamo τ(σ^(−1)(e)) = σ^(−1)(e). Quindi:

(σ τ σ^(−1))(e) = σ(σ^(−1)(e)) = e

Quindi σ τ σ^(−1) fissa e, e poiché e era arbitrario, σ τ σ^(−1) ∈ Gal(L/E).

(⟸) Supponiamo Gal(L/E) normale in G. Dobbiamo mostrare che E/K è normale.

Sia p(x) ∈ K[x] irriducibile con una radice α ∈ E. Dobbiamo mostrare che tutte le radici di p(x) stanno in E.

Sia β un'altra radice di p(x) in L. Poiché p(x) è il polinomio minimo di entrambi α e β, esiste un K-isomorfismo K(α) → K(β) che manda α in β. Questo si estende a un K-automorfismo σ di L (perché L/K è normale).

Quindi σ ∈ G = Gal(L/K) e σ(α) = β. Vogliamo mostrare β ∈ E, cioè σ(α) ∈ E.

Sia τ ∈ Gal(L/E). Poiché α ∈ E, abbiamo τ(α) = α. Consideriamo σ^(−1) τ σ. Per la normalità di Gal(L/E), questo elemento sta in Gal(L/E), quindi:

(σ^(−1) τ σ)(α) = α

Applicando σ:

$\tau(\sigma(\alpha)) = \sigma(\alpha)$

Quindi $\sigma(\alpha)$ è fissato da ogni $\tau \in Gal(L/E)$, il che significa $\sigma(\alpha) \in L^{(Gal(L/E)) = E}$.

Infine, per l'isomorfismo $Gal(E/K) \cong G/Gal(L/E)$, definiamo la mappa di restrizione:

$\varphi: G \to Gal(E/K)$ $\sigma \mapsto \sigma|_E$ (restrizione di σ a E)

Questa è un omomorfismo suriettivo di gruppi con nucleo Gal(L/E). Per il primo teorema di isomorfismo:

$G/Gal(L/E) \cong Gal(E/K)$

I

3.2 Esempio Fondamentale: $Q(\sqrt[4]{2}, i)/Q$

Illustriamo il teorema fondamentale con l'esempio $Q(\sqrt[4]{2}, i)/Q$.

Abbiamo visto che $G = Gal(Q(\sqrt[4]{2}, i)/Q) \cong D_4$, il gruppo diedrale di ordine 8. Gli elementi sono:

- id: identità
- τ: rotazione che manda $\sqrt[4]{2} \mapsto i\cdot\sqrt[4]{2}$, $i \mapsto i$
- τ^2: manda $\sqrt[4]{2} \mapsto -\sqrt[4]{2}$, $i \mapsto i$
- τ^3: manda $\sqrt[4]{2} \mapsto -i\cdot\sqrt[4]{2}$, $i \mapsto i$
- ρ: coniugazione complessa, fissa $\sqrt[4]{2}$, manda $i \mapsto -i$
- $\tau\rho$, $\tau^2\rho$, $\tau^3\rho$: composizioni

La struttura del gruppo:

- $\tau^4 = id$, quindi $\langle\tau\rangle \cong Z/4Z$
- $\rho^2 = id$, quindi $\langle\rho\rangle \cong Z/2Z$
- $\rho\tau\rho = \tau^3$ (relazione di non commutatività)

Sottogruppi di D_4:

1. {id} (ordine 1)
2. $\langle\tau\rangle = \{id, \tau, \tau^2, \tau^3\}$ (ordine 4, ciclico)
3. $\langle\tau^2\rangle = \{id, \tau^2\}$ (ordine 2)
4. $\langle\tau^2\rho\rangle = \{id, \tau^2\rho\}$ (ordine 2)
5. $\langle\rho\rangle = \{id, \rho\}$ (ordine 2)
6. $\langle\tau\rho\rangle = \{id, \tau\rho\}$ (ordine 2)
7. $\langle\tau^3\rho\rangle = \{id, \tau^3\rho\}$ (ordine 2)
8. $\langle\tau^2, \rho\rangle = \{id, \tau^2, \rho, \tau^2\rho\}$ (ordine 4, non ciclico, $\cong Z/2Z \times Z/2Z$)
9. $\langle\tau^2, \tau\rho\rangle = \{id, \tau^2, \tau\rho, \tau^3\rho\}$ (ordine 4)
10. D_4 stesso (ordine 8)

Campi intermedi corrispondenti:

Per ogni sottogruppo H, il campo fisso L^H è:

1. L^({id}) = Q(⁴√2, i) (campo totale)

2. L^(⟨τ⟩): elementi fissati da tutte le rotazioni. Solo gli elementi di Q(i) sono fissati (perché τ permuta le potenze di ⁴√2 ma fissa i). Quindi L^(⟨τ⟩) = Q(i) Verifica: [Q(⁴√2, i):Q(i)] = |⟨τ⟩| = 4 ✓

3. L^(⟨τ²⟩): fissato da τ² che manda ⁴√2 ↦ −⁴√2. Gli elementi fissati sono quelli che contengono solo potenze pari di ⁴√2, cioè Q(√2, i). [Q(⁴√2, i):Q(√2, i)] = 2 ✓

4. L^(⟨τ²ρ⟩): τ²ρ manda ⁴√2 ↦ −⁴√2 e i ↦ −i. Gli elementi fissati formano Q(√2). [Q(⁴√2, i):Q(√2)] = 4 ✓

5. L^(⟨ρ⟩): ρ è la coniugazione complessa, fissa i reali. Quindi L^(⟨ρ⟩) = Q(⁴√2). [Q(⁴√2, i):Q(⁴√2)] = 2 ✓

6. L^(⟨τρ⟩): τρ manda ⁴√2 ↦ i·⁴√2 e i ↦ −i. Fissiamo elementi del tipo a + b(⁴√2 + (−i)·⁴√2) = a + b·⁴√2(1 − i). Campo: Q(⁴√2(1 − i))

7. L^(⟨τ³ρ⟩): analogamente, Q(⁴√2(1 + i))

8. L^(⟨τ², ρ⟩): intersezione di Q(√2, i) e Q(⁴√2), che è Q(√2). Questo sottogruppo è normale (è il centro di D_4), quindi Q(√2)/Q è normale. ✓

9. L^(⟨τ², τρ⟩): simile analisi porta a un altro campo quadratico.

10. L^(D_4) = Q (campo base) [Q(⁴√2, i):Q] = |D_4| = 8 ✓

Sottogruppi normali e estensioni normali:

I sottogruppi normali di D_4 sono:

- {id} (banale)
- ⟨τ²⟩ = {id, τ²}
- ⟨τ⟩ = {id, τ, τ², τ³}
- D_4 (tutto)

I campi corrispondenti danno estensioni normali su Q:

- Q(⁴√2, i)/Q è normale (ovviamente)
- Q(√2, i)/Q è normale (campo di spezzamento di (x² − 2)(x² + 1))
- Q(i)/Q è normale (campo di spezzamento di x² + 1)
- Q/Q è normale (banale)

Mentre Q(⁴√2)/Q NON è normale (⟨ρ⟩ non è normale in D_4), corrispondentemente il polinomio x⁴ − 2 non si spezza completamente in Q(⁴√2).

Capitolo 4: Equazioni Polinomiali e Risolubilità per Radicali

Il problema originale che motivò Galois era determinare quali equazioni polinomiali possono essere risolte mediante radicali. La teoria che abbiamo sviluppato fornisce la risposta completa.

4.1 Estensioni Radicali

Definizione: Un'estensione L/K è detta estensione radicale se esiste una torre di campi:

$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq ... \subseteq K_n = L$

tale che per ogni i = 1, ..., n, l'estensione $K_i/K_{(i-1)}$ è ottenuta aggiungendo una radice n_i-esima, cioè esiste $\alpha_i \in K_i$ tale che $\alpha_i^{(n_i)} \in K_{(i-1)}$ e $K_i = K_{(i-1)}(\alpha_i)$.

In altre parole, ogni passo nella torre è ottenuto estraendo una radice.

Esempi:

1. $Q(\sqrt{2})/Q$ è radicale: una sola torre con $K_0 = Q$, $K_1 = Q(\sqrt{2})$, dove $(\sqrt{2})^2 = 2 \in Q$.
2. $Q(\sqrt[4]{2}, i)/Q$ è radicale: $Q \subseteq Q(i) \subseteq Q(i, \sqrt[4]{2})$ dove $i^2 = -1 \in Q$ e $(\sqrt[4]{2})^4 = 2 \in Q(i)$.
3. Il campo di spezzamento di $x^5 - x - 1$ su Q NON è radicale (come dimostreremo).

Definizione: Un polinomio $p(x) \in K[x]$ è detto risolubile per radicali su K se esiste un'estensione radicale L/K tale che p(x) si spezza completamente in L[x].

Equivalentemente, tutte le radici di p(x) possono essere espresse mediante radicali a partire dai coefficienti.

4.2 Gruppi Risolubili

Il concetto chiave che collega le estensioni radicali alla teoria dei gruppi è quello di gruppo risolubile.

Definizione: Un gruppo G è detto risolubile se esiste una serie normale:

$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq ... \trianglelefteq G_n = G$

dove ogni quoziente $G_{(i+1)}/G_i$ è abeliano.

Una serie normale è una catena di sottogruppi dove ogni G_i è normale in $G_{(i+1)}$.

Esempi:

1. Ogni gruppo abeliano è risolubile: la serie $\{e\} \trianglelefteq G$ ha un solo quoziente $G/\{e\} \cong G$ che è abeliano.

2. Il gruppo simmetrico S_3 è risolubile: $\{e\} \trianglelefteq A_3 \trianglelefteq S_3$ dove $A_3 = \{e, (123), (132)\}$ è il sottogruppo alterno (permutazioni pari). Abbiamo:

    - $A_3/\{e\} \cong A_3 \cong \mathbb{Z}/3\mathbb{Z}$ (abeliano)
    - $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$ (abeliano)
3. Il gruppo diedrale D_4 è risolubile: $\{e\} \trianglelefteq \langle \tau^2 \rangle \trianglelefteq \langle \tau \rangle \trianglelefteq D_4$ I quozienti sono:

    - $\langle \tau^2 \rangle/\{e\} \cong \mathbb{Z}/2\mathbb{Z}$
    - $\langle \tau \rangle/\langle \tau^2 \rangle \cong \mathbb{Z}/2\mathbb{Z}$
    - $D_4/\langle \tau \rangle \cong \mathbb{Z}/2\mathbb{Z}$ Tutti abeliani.
4. Il gruppo simmetrico S_5 NON è risolubile. Più in generale, S_n non è risolubile per $n \geq 5$.

Proposizione: Sottogruppi e quozienti di gruppi risolubili sono risolubili.

Dimostrazione:

Sottogruppi: Sia $H \subseteq G$ con G risolubile. Consideriamo una serie normale di G:

$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_n = G$

Definiamo $H_i = H \cap G_i$. Allora:

$\{e\} = H_0 \subseteq H_1 \subseteq ... \subseteq H_n = H$

Ogni H_i è normale in $H_{(i+1)}$. Per il secondo teorema di isomorfismo:

$H_{(i+1)}/H_i \cong (H_{(i+1)} \cdot G_i)/G_i \subseteq G_{(i+1)}/G_i$

Poiché $G_{(i+1)}/G_i$ è abeliano, anche il suo sottogruppo $H_{(i+1)}/H_i$ è abeliano.

Quozienti: Sia G risolubile e $N \trianglelefteq G$. Consideriamo la proiezione $\pi: G \to G/N$. L'immagine di una serie normale di G è una serie normale di G/N, e i quozienti rimangono abeliani. ∎

4.3 Teorema di Galois sulla Risolubilità

Il risultato centrale che collega tutto insieme è:

Teorema di Galois: Sia K un campo di caratteristica zero e $p(x) \in K[x]$ un polinomio. Sia L il campo di spezzamento di p(x) su K. Allora p(x) è risolubile per radicali su K se e solo se Gal(L/K) è un gruppo risolubile.

Questo teorema fornisce un criterio puramente algebrico (la risolubilità del gruppo di Galois) per una questione analitica (l'esprimibilità delle radici mediante radicali).

Dimostrazione (schema delle idee principali):

($\Rightarrow$) Supponiamo p(x) risolubile per radicali. Allora esiste un'estensione radicale M/K tale che $L \subseteq M$.

Possiamo assumere che M/K sia galoisiana (eventualmente passando a una chiusura normale). La torre radicale per M può essere scritta come:

$K = K_0 \subseteq K_1 \subseteq ... \subseteq K_n = M$

dove $K_{i+1} = K_i(\alpha_{i+1})$ con $\alpha_{i+1}^{m_{i+1}} \in K_i$.

Se char(K) = 0, possiamo assumere che K contenga tutte le radici m_i-esime dell'unità (aggiungendole se necessario, il che non cambia la risolubilità).

Sotto queste ipotesi, ogni estensione K_{i+1}/K_i è ciclica (estensione di Kummer). Per la teoria di Kummer, il gruppo di Galois $Gal(K_{i+1}/K_i)$ è abeliano.

Consideriamo ora la torre ristretta a L:

$K = L_0 \subseteq L_1 \subseteq ... \subseteq L_r = L$

dove $L_i = L \cap K_i$. Per il teorema fondamentale, questa torre corrisponde a una serie di sottogruppi:

$Gal(L/K) = H_r \supseteq H_{r-1} \supseteq ... \supseteq H_0 = \{e\}$

dove $H_i = Gal(L/L_i)$. I quozienti H_i/H_{i+1} sono quozienti di gruppi abeliani (perché sono quozienti di $Gal(K_{i+1}/K_i)$), quindi sono abeliani.

Quindi Gal(L/K) è risolubile.

($\Leftarrow$) Supponiamo Gal(L/K) risolubile. Dobbiamo mostrare che L può essere ottenuto da K mediante estensioni radicali.

Sia G = Gal(L/K) con una serie normale:

$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_n = G$

dove ogni G_{i+1}/G_i è abeliano. Per il teorema fondamentale, questa corrisponde a una torre di campi:

$K = L_n \subseteq L_{n-1} \subseteq ... \subseteq L_0 = L$

dove $L_i = L^{G_i}$.

Ogni estensione L_{i-1}/L_i è galoisiana con gruppo di Galois G_i/G_{i+1}, che è abeliano.

Aggiungendo le opportune radici dell'unità, possiamo applicare la teoria di Kummer per mostrare che ogni estensione abeliana può essere ottenuta mediante radicali.

Quindi L può essere ottenuto da K mediante una torre radicale. ∎

4.4 Non Risolubilità del Quintico Generale

Ora possiamo finalmente rispondere alla domanda millenaria: perché non esiste una formula generale per le equazioni di quinto grado?

Teorema (Abel-Ruffini): Il polinomio generale di grado 5:

$p(x) = x^5 + a_1 x^4 + a_2 x^3 + a_3 x^2 + a_4 x + a_5$

non è risolubile per radicali su $K = Q(a_1, a_2, a_3, a_4, a_5)$.

Dimostrazione: Il campo di spezzamento di p(x) su K ha gruppo di Galois S_5, il gruppo simmetrico su 5 elementi.

Infatti, le cinque radici $x_1, ..., x_5$ sono algebricamente indipendenti su Q, e ogni permutazione delle radici estende a un automorfismo del campo di spezzamento che fissa K (perché i coefficienti a_i sono le funzioni simmetriche elementari delle radici, che sono invarianti sotto permutazioni).

Dobbiamo mostrare che S_5 non è risolubile.

Lemma: S_n non è risolubile per $n \geq 5$.

Dimostrazione del lemma: Supponiamo per assurdo che S_5 sia risolubile. Sia:

$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_r = S_5$

una serie normale con quozienti abeliani.

L'unico sottogruppo normale non banale di S_5 è A_5, il gruppo alterno (questo è un fatto noto della teoria dei gruppi). Quindi deve apparire A_5 nella serie.

Sia $G_i = A_5$ per qualche i. Allora $G_{i-1} \trianglelefteq A_5$.

Ma A_5 è un gruppo semplice, cioè i suoi unici sottogruppi normali sono {e} e A_5 stesso. Quindi $G_{i-1} = \{e\}$.

Questo significa che $A_5/G_{i-1} = A_5/\{e\} \cong A_5$ è abeliano. Ma A_5 non è abeliano (ad esempio, (12)(34) e (123) non commutano).

Contraddizione. Quindi S_5 non è risolubile. ∎

Per il teorema di Galois, il polinomio generale di grado 5 non è risolubile per radicali. ∎

Osservazione importante: Questo non significa che NESSUN polinomio di grado 5 sia risolubile per radicali. Significa solo che non esiste una formula generale che funzioni per tutti i polinomi di grado 5.

Esempi di polinomi di grado 5 risolubili:

1. $x^5 - 1 = 0$: le soluzioni sono le radici quinte dell'unità, tutte esprimibili mediante radicali.

2. $x^5 - x - 1 = 0$: il gruppo di Galois è S_5, quindi NON risolubile per radicali.

3. $x^5 - 5x + 12 = 0$: il gruppo di Galois è F_20, il gruppo di Frobenius di ordine 20, che è risolubile. Quindi questo polinomio è risolubile per radicali (anche se la formula esplicita è estremamente complicata).

4.5 Le Formule Classiche per i Gradi Bassi

Per completezza, ricordiamo le formule risolutive per i gradi 2, 3, 4.

Grado 2: $ax^2 + bx + c = 0$

$x = (-b \pm \sqrt{(b^2 - 4ac)}) / (2a)$

Il gruppo di Galois (nel caso generale) è S_2 ≅ Z/2Z, che è abeliano quindi risolubile.

Grado 3: $x^3 + px + q = 0$ (forma ridotta)

Formula di Cardano:

$x = \sqrt[3]{(-q/2 + \sqrt{(q^2/4 + p^3/27)})} + \sqrt[3]{(-q/2 - \sqrt{(q^2/4 + p^3/27)})}$

Il discriminante è $\Delta = -4p^3 - 27q^2$. Il gruppo di Galois è:

- S_3 se Δ non è un quadrato perfetto
- A_3 ≅ Z/3Z se Δ è un quadrato perfetto

Entrambi sono risolubili.

Grado 4: Il metodo di Ferrari riduce l'equazione di quarto grado a una di terzo grado (la risolvente cubica), che può essere risolta con Cardano.

Il gruppo di Galois può essere S_4, A_4, D_4, V_4 (gruppo di Klein), Z/4Z, o Z/2Z × Z/2Z. Tutti questi sono risolubili.

Capitolo 5: Campi Finiti e Teoria di Galois

I campi finiti hanno un ruolo centrale nelle applicazioni crittografiche della teoria di Galois. La loro struttura è particolarmente semplice e completamente compresa.

5.1 Struttura dei Campi Finiti

Teorema fondamentale sui campi finiti:

1. Per ogni numero primo p e ogni intero positivo n, esiste un unico (a meno di isomorfismo) campo con p^n elementi, denotato F_(p^n) o GF(p^n).

2. Ogni campo finito ha cardinalità p^n per qualche primo p e qualche n ≥ 1.

3. F_(p^n) è il campo di spezzamento del polinomio x^(p^n) − x su F_p.

Dimostrazione:

(3) ⟹ (1) (Esistenza e unicità): Il campo di spezzamento di x^(p^n) − x su F_p esiste ed è unico. Chiamiamolo L. Dobbiamo mostrare che |L| = p^n.

Le radici di x^(p^n) − x sono esattamente gli elementi α ∈ $\bar{L}$ (chiusura algebrica di F_p) tali che α^(p^n) = α.

Affermiamo che l'insieme S = {α ∈ $\bar{L}$: α^(p^n) = α} è un sottocampo di $\bar{L}$.

- 0, 1 ∈ S (ovvio)
- Se α, β ∈ S, allora (α + β)^(p^n) = α^(p^n) + β^(p^n) = α + β (usando il fatto che in caratteristica p, (a+b)^p = a^p + b^p)
- Se α, β ∈ S, allora (αβ)^(p^n) = α^(p^n) β^(p^n) = αβ
- Se α ∈ S con α ≠ 0, allora α^(p^n) = α implica (α^(−1))^(p^n) = α^(−1)

Quindi S è un campo. Poiché L è il campo di spezzamento di x^(p^n) − x, abbiamo L = S.

Il polinomio x^(p^n) − x ha al massimo p^n radici in $\bar{L}$ (perché $\bar{L}$ è un campo, quindi un dominio di integrità). Ma la derivata è:

(x^(p^n) − x)' = p^n x^(p^n−1) − 1 = −1 ≠ 0

Quindi x^(p^n) − x non ha radici multiple. Quindi ha esattamente p^n radici distinte, quindi |L| = p^n.

(2) (Struttura generale): Sia F un campo finito. Sia p la caratteristica di F (che deve essere un numero primo). Allora F contiene F_p come sottocampo.

Quindi F è uno spazio vettoriale su F_p di dimensione finita, diciamo n. Quindi:

|F| = |F_p|^n = p^n

(1) (Unicità generale): Se F e F' sono due campi con p^n elementi, entrambi sono campi di spezzamento di x^(p^n) − x su F_p, quindi sono F_p-isomorfi. ∎

5.2 L'Automorfismo di Frobenius

Definizione: Sia F un campo di caratteristica p > 0. L'automorfismo di Frobenius è la mappa:

φ: F → F φ(x) = x^p

Proposizione: φ è un omomorfismo di campi.

Dimostrazione:

φ(xy) = (xy)^p = x^p y^p = φ(x) φ(y)

φ(x + y) = (x + y)^p = Σ_(k=0)^p (p choose k) x^k y^(p−k)

Ma (p choose k) = p! / (k!(p−k)!) è divisibile per p per 0 < k < p (perché p è primo e appare al numeratore ma non al denominatore). Quindi in caratteristica p:

(p choose k) ≡ 0 (mod p) per 0 < k < p

Quindi φ(x + y) = x^p + y^p = φ(x) + φ(y).

Inoltre, φ(1) = 1^p = 1, quindi φ è un omomorfismo di anelli unitari. Poiché F è un campo, φ è iniettivo (il nucleo di un omomorfismo di campi è sempre banale o tutto il campo). Se F è finito, φ è anche suriettivo, quindi è un automorfismo. ∎

Teorema (Gruppo di Galois dei campi finiti): Per ogni campo finito F_(p^n), il gruppo di Galois Gal(F_(p^n)/F_p) è ciclico di ordine n, generato dall'automorfismo di Frobenius φ(x) = x^p.

Dimostrazione:

Sappiamo che F_(p^n) è il campo di spezzamento di x^(p^n) − x su F_p, quindi l'estensione è galoisiana e [F_(p^n):F_p] = n.

L'automorfismo di Frobenius φ soddisfa:

- φ fissa F_p (perché per ogni a ∈ F_p, abbiamo a^p = a per il piccolo teorema di Fermat)
- φ^n(x) = x^(p^n) = x per ogni x ∈ F_(p^n) (perché ogni elemento di F_(p^n) è radice di x^(p^n) − x)

Quindi φ ∈ Gal(F_(p^n)/F_p) e l'ordine di φ divide n.

Supponiamo che φ^k = id per qualche k < n. Allora x^(p^k) = x per ogni x ∈ F_(p^n), il che significa che F_(p^n) è contenuto nel campo di spezzamento di x^(p^k) − x, che ha al massimo p^k elementi. Ma |F_(p^n)| = p^n > p^k, contraddizione.

Quindi l'ordine di φ è esattamente n. Poiché |Gal(F_(p^n)/F_p)| = n, il sottogruppo ciclico generato da φ è tutto il gruppo. ∎

Corollario: F_(p^m) ⊆ F_(p^n) (come sottocampi) se e solo se m divide n.

Dimostrazione:

(⟹) Se F_(p^m) ⊆ F_(p^n), allora per la formula della torre:

[F_(p^n):F_p] = [F_(p^n):F_(p^m)] · [F_(p^m):F_p]

Quindi n = [F_(p^n):F_(p^m)] · m, quindi m divide n.

(⇐) Se m divide n, diciamo n = mk, allora φ^m genera un sottogruppo di ordine k di Gal(F_(p^n)/F_p). Per il teorema fondamentale, questo corrisponde a un campo intermedio E con [E:F_p] = m. Quindi E ≅ F_(p^m). ▮

Esempio concreto: Consideriamo F_4 = F_(2²).

Come insieme, F_4 = {0, 1, α, α+1} dove α è una radice del polinomio irriducibile x² + x + 1 ∈ F_2[x].

Le operazioni sono definite modulo x² + x + 1, quindi α² = α + 1.

Tabelle di addizione e moltiplicazione:

```
+ | 0  1  α  α+1        · | 0  1  α  α+1
---+-------------      ---+-------------
0  | 0  1  α  α+1       0  | 0  0  0  0
1  | 1  0 α+1  α        1  | 0  1  α  α+1
α  | α α+1 0  1         α  | 0  α α+1 1
α+1|α+1 α  1  0         α+1| 0 α+1 1  α
```

L'automorfismo di Frobenius φ: x ↦ x² mappa:

- φ(0) = 0
- φ(1) = 1
- φ(α) = α² = α + 1
- φ(α+1) = (α+1)² = α² + 2α + 1 = α² + 1 = (α+1) + 1 = α

Quindi φ scambia α e α+1. Verificando: φ² = id, e Gal(F_4/F_2) = {id, φ} ≅ Z/2Z. ✓

5.3 Polinomi Irriducibili su Campi Finiti

Definizione: Un polinomio f(x) ∈ F_q[x] di grado n è irriducibile se non può essere fattorizzato in prodotto di polinomi di grado inferiore in F_q[x].

Teorema: Un polinomio f(x) ∈ F_q[x] di grado n è irriducibile se e solo se:

1. f(x) divide x^(q^n) − x
2. gcd(f(x), x^(q^m) − x) = 1 per ogni divisore proprio m di n

Dimostrazione:

(⇒) Se f(x) è irriducibile di grado n, sia α una radice di f(x) in una chiusura algebrica. Allora F_q(α) ≅ F_q[x]/(f(x)) ha q^n elementi, quindi è isomorfo a F_(q^n).

Ogni elemento di F_(q^n) è radice di x^(q^n) − x, quindi α è radice di x^(q^n) − x, quindi f(α) = 0 implica che f(x) divide x^(q^n) − x.

Se m < n è un divisore proprio di n, allora F_(q^m) è un sottocampo proprio di F_(q^n) = F_q(α), quindi α ∉ F_(q^m), quindi α non è radice di x^(q^m) − x, quindi f(x) non divide x^(q^m) − x.

(⇐) Supponiamo che f(x) soddisfi (1) e (2). Sia α una radice di f(x). Allora α ∈ F_(q^n) perché f(x) divide x^(q^n) − x.

Quindi [F_q(α):F_q] divide [F_(q^n):F_q] = n. Sia d = [F_q(α):F_q] = deg(f), il grado del polinomio minimo di α.

Allora α ∈ F_(q^d) ⊆ F_(q^n), quindi d divide n. Ma α è radice di x^(q^d) − x, quindi f(α) = 0 implica che f(x) e x^(q^d) − x hanno α come radice comune. Se d < n, questo contraddirebbe (2).

Quindi d = n = deg(f), quindi f(x) è il polinomio minimo di α, quindi è irriducibile. ∎

Teorema (Numero di polinomi irriducibili): Il numero di polinomi monici irriducibili di grado n su F_q è:

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu(n/d)\, q^d$$

dove μ è la funzione di Möbius.

Dimostrazione: Usiamo la formula di inversione di Möbius.

Sia M(n) il numero di elementi di F_(q^n) con polinomio minimo di grado esattamente n su F_q. Chiaramente:

$$q^n = \sum_{d|n} M(d)$$

perché ogni elemento di F_(q^n) ha polinomio minimo di grado d per qualche divisore d di n.

Per inversione di Möbius:

$$M(n) = \sum_{d|n} \mu(n/d)\, q^d$$

Ora, ogni polinomio monico irriducibile di grado n ha esattamente n radici distinte in F_(q^n) (le radici sono α, α^q, α^(q²), ..., α^(q^(n−1)), tutte distinte e tutte con lo stesso polinomio minimo). Quindi:

$$M(n) = n \cdot N_q(n)$$

da cui:

$$N_q(n) = M(n)/n = \frac{1}{n} \sum_{d|n} \mu(n/d)\, q^d$$

∎

Esempio: Numero di polinomi irriducibili di grado 3 su F_2:

$$N_2(3) = \frac{1}{3}[\mu(3)\cdot 2^1 + \mu(1)\cdot 2^3] = \frac{1}{3}[(-1)\cdot 2 + 1\cdot 8] = \frac{1}{3}[-2 + 8] = 6/3 = 2$$

Infatti, i due polinomi irriducibili di grado 3 su F_2 sono $x^3 + x + 1$ e $x^3 + x^2 + 1$.

Verifica: $x^3 + x^2 + x + 1 = (x+1)(x^2+1)$ è riducibile, e $x^3 = x \cdot x^2$ è riducibile, ecc.

5.4 Radici Primitive e Generatori

Definizione: Sia F_q un campo finito. Un elemento $\alpha \in F_q^* = F_q \setminus \{0\}$ è detto radice primitiva o generatore se il suo ordine moltiplicativo è $q - 1$, cioè se $\alpha^{(q-1)} = 1$ ma $\alpha^k \neq 1$ per $0 < k < q - 1$.

Equivalentemente, α genera l'intero gruppo moltiplicativo F_q^*.

Teorema: Il gruppo moltiplicativo F_q^* di un campo finito è ciclico di ordine $q - 1$.

Dimostrazione:

Per il teorema di struttura dei gruppi abeliani finiti, F_q^* è isomorfo a un prodotto di gruppi ciclici:

$F_q^* \cong Z_{n_1} \times Z_{n_2} \times ... \times Z_{n_k}$

dove n_{i+1} divide n_i per ogni i.

Sia $m = n_1$ il massimo degli ordini degli elementi. Allora ogni elemento di F_q^* soddisfa $x^m = 1$, cioè ogni elemento è radice del polinomio $x^m - 1$.

Ma un polinomio di grado m ha al massimo m radici in un campo. Quindi:

$q - 1 = |F_q^*| \leq m$

D'altra parte, esiste un elemento di ordine m, quindi m divide $|F_q^*| = q - 1$. Quindi $m = q - 1$.

Questo significa che esiste un elemento di ordine $q - 1$, quindi F_q^* è ciclico. ∎

Corollario: Il numero di generatori di F_q^* è $\varphi(q - 1)$, dove φ è la funzione totiente di Eulero.

Esempio: $F_7^* = \{1, 2, 3, 4, 5, 6\}$ ha $\varphi(6) = 2$ generatori.

Verifichiamo:

- $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$. Quindi 3 è un generatore.
- $5^1 = 5$, $5^2 = 4$, $5^3 = 6$, $5^4 = 2$, $5^5 = 3$, $5^6 = 1$. Quindi 5 è un generatore.
- $2^3 = 1$, quindi 2 non è un generatore (ha ordine 3).
- $4^2 = 2$, $4^3 = 1$, quindi 4 ha ordine 3.
- $6^2 = 1$, quindi 6 ha ordine 2.

I generatori sono 3 e 5. ✓

Capitolo 6: Applicazioni Crittografiche della Teoria di Galois

La teoria di Galois ha applicazioni profonde e dirette nella crittografia moderna. I campi finiti e le loro estensioni sono il fondamento matematico di numerosi algoritmi crittografici.

6.1 Aritmetica nei Campi di Galois GF(2^n)

I campi della forma GF(2^n) sono particolarmente importanti in crittografia perché i loro elementi possono essere rappresentati come stringhe di bit, e le operazioni possono essere implementate efficientemente in hardware e software.

Rappresentazione polinomiale: Gli elementi di GF(2^n) possono essere rappresentati come polinomi di grado < n con coefficienti in GF(2) = {0, 1}, modulo un polinomio irriducibile fisso p(x) di grado n.

Ad esempio, in $GF(2^8)$ (usato nell'AES), se scegliamo $p(x) = x^8 + x^4 + x^3 + x + 1$, allora ogni elemento può essere scritto come:

$a = a_7\, x^7 + a_6\, x^6 + ... + a_1\, x + a_0$

dove $a_i \in \{0, 1\}$. Questo può essere rappresentato come il byte [a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0] in notazione binaria, o come un intero tra 0 e 255.

Operazioni fondamentali:

1. **Addizione**: È semplicemente XOR bit a bit.

   Se $a = \Sigma\, a_i\, x^i$ e $b = \Sigma\, b_i\, x^i$, allora:

   $a + b = \Sigma\, (a_i \oplus b_i)\, x^i$

   dove $\oplus$ denota XOR.

   Esempio in $GF(2^8)$:

   - $57_{16} = 01010111_2$ rappresenta $x^6 + x^4 + x^2 + x + 1$
   - $83_{16} = 10000011_2$ rappresenta $x^7 + x + 1$
   - $57_{16} \oplus 83_{16} = D4_{16} = 11010100_2$ rappresenta $x^7 + x^6 + x^4 + x^2$

Moltiplicazione: È moltiplicazione polinomiale seguita da riduzione modulo p(x).

Algoritmo shift-and-add:

```
function multiply(a, b, p):
  result = 0
  for i from 0 to n-1:
    if (b & 1) == 1:
```

```
        result = result ⊕ a
    carry = (a & (1 << (n-1))) != 0
    a = a << 1
    if carry:
        a = a ⊕ p
    b = b >> 1
return result
```

2.
3. **Inversione**: Per calcolare a^(−1) in GF(2^n), possiamo usare:

    - L'algoritmo euclideo esteso sui polinomi
    - Esponenziazione veloce: a^(−1) = a^(2^n − 2) (perché a^(2^n − 1) = 1 per il piccolo teorema di Fermat)
    - Tabelle pre-calcolate per campi piccoli

Esempio dettagliato in GF(2^8):

Consideriamo la moltiplicazione di 57_{16} per 83_{16} in GF(2^8) con $p(x) = x^8 + x^4 + x^3 + x + 1$ (polinomio usato nell'AES).

$57_{16} = x^6 + x^4 + x^2 + x + 1$ $83_{16} = x^7 + x + 1$

Moltiplichiamo come polinomi:

$(x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1) = x^{13} + x^7 + x^6 + x^{11} + x^5 + x^4 + x^9 + x^3 + x^2 + x^8 + x^2 + x + x^7 + x + 1 = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \pmod 2$

Ora riduciamo modulo $p(x) = x^8 + x^4 + x^3 + x + 1$:

$x^{13} \bmod p(x)$: dividiamo x^{13} per x^8 ottenendo quoziente x^5 $x^{13} = x^5 \cdot (x^8 + x^4 + x^3 + x + 1) + (x^9 + x^8 + x^6 + x^5)$ Quindi $x^{13} \equiv x^9 + x^8 + x^6 + x^5 \pmod{p(x)}$

Continuando sistematicamente:

Risultato finale: $C1_{16} = 11000001_2 = x^7 + x^6 + 1$

Questa è l'operazione fondamentale usata nella S-box dell'AES.

6.2 L'Advanced Encryption Standard (AES) e GF(2^8)

L'AES è il cifrario a blocchi standard approvato dal NIST nel 2001, sostituendo il DES. La sua sicurezza si basa fortemente sull'aritmetica in GF(2^8).

Struttura dell'AES:

L'AES opera su blocchi di 128 bit, organizzati come una matrice 4×4 di byte (chiamata stato). Il numero di round dipende dalla lunghezza della chiave:

- AES-128: 10 round (chiave 128 bit)

- AES-192: 12 round (chiave 192 bit)
- AES-256: 14 round (chiave 256 bit)

Ogni round (eccetto l'ultimo) consiste di quattro trasformazioni:

1. **SubBytes** (Sostituzione non lineare)
2. **ShiftRows** (Permutazione)
3. **MixColumns** (Diffusione)
4. **AddRoundKey** (Combinazione con la chiave di round)

SubBytes e l'inversione in GF(2^8):

La trasformazione SubBytes è l'unica componente non lineare dell'AES ed è cruciale per la sua sicurezza. Per ogni byte dello stato, SubBytes applica:

1. Calcola l'inverso moltiplicativo in GF(2^8): se l'input è b, calcola b' = b^(−1) (con la convenzione che 0^(−1) = 0)

2. Applica una trasformazione affine su GF(2):

   b'i = $b'i \oplus b'((i+4) \bmod 8) \oplus b'$((i+5) mod 8) ⊕ b'$((i+6) \bmod 8) \oplus b'$((i+7) mod 8) ⊕ c_i

   dove c = 63_{16} = 01100011_2

La trasformazione inversa in GF(2^8) fornisce la non linearità. L'inverso moltiplicativo in un campo finito è una funzione altamente non lineare che non può essere approssimata bene da funzioni lineari o affini.

Proprietà crittografiche della S-box:

La S-box dell'AES è progettata per avere:

1. **Alta non linearità**: Misurata dalla distanza di Hamming minima dalla funzione affine più vicina. La S-box dell'AES ha non linearità 112, vicina al massimo teorico di 120 per funzioni da 8 bit a 8 bit.

2. **No fixed points**: S(x) ≠ x per ogni x ≠ 0

3. **No opposite fixed points**: S(x) ≠ x ⊕ FF_{16} per ogni x

4. **Branch number ottimale**: Per resistere agli attacchi differenziali e lineari

Tutte queste proprietà derivano dalla struttura algebrica di GF(2^8) e dalla scelta attenta del polinomio irriducibile.

MixColumns e la moltiplicazione polinomiale:

La trasformazione MixColumns interpreta ogni colonna dello stato come un polinomio di grado < 4 con coefficienti in $GF(2^8)$ e la moltiplica modulo $x^4 + 1$ per il polinomio fisso:

$c(x) = 03 \cdot x^3 + 01 \cdot x^2 + 01 \cdot x + 02$

in notazione esadecimale, dove i coefficienti sono elementi di $GF(2^8)$.

In forma matriciale:

[b_0]   [02 03 01 01] [a_0]
[b_1] = [01 02 03 01] [a_1]
[b_2]   [01 01 02 03] [a_2]
[b_3]   [03 01 01 02] [a_3]

dove tutte le moltiplicazioni e addizioni sono in $GF(2^8)$.

Questa matrice è una matrice MDS (Maximum Distance Separable), che garantisce ottima diffusione: un cambiamento in un byte di input causa cambiamenti in tutti e quattro i byte di output.

Teorema: La matrice MixColumns di AES ha branch number 5, il massimo possibile per una matrice 4×4 su $GF(2^8)$.

Il branch number è definito come il minimo su tutti i vettori di input non nulli di:

$BN = peso(x) + peso(M \cdot x)$

dove peso(x) è il numero di componenti non nulle. Un branch number di 5 significa che input e output insieme hanno almeno 5 byte attivi, fornendo forte diffusione.

6.3 Curve Ellittiche su Campi Finiti

Le curve ellittiche definite su campi finiti sono fondamentali nella crittografia moderna. La teoria di Galois gioca un ruolo cruciale nella loro comprensione.

Definizione: Una curva ellittica su un campo finito F_q (con q dispari) è data dall'equazione:

$E: y^2 = x^3 + ax + b$

dove $a, b \in F_q$ soddisfano $4a^3 + 27b^2 \neq 0$ (condizione di non singolarità).

Per q = 2^n, si usa spesso la forma:

$E: y^2 + xy = x^3 + ax^2 + b$

Il gruppo di punti $E(F_q)$:

L'insieme $E(F_q) = \{(x, y) \in F_q \times F_q : y^2 = x^3 + ax + b\} \cup \{O\}$ forma un gruppo abeliano sotto l'operazione di addizione geometrica.

Teorema di Hasse: Il numero di punti su E(F_q) soddisfa:

$|E(F_q)| = q + 1 - t$

dove $|t| \leq 2\sqrt{q}$. Il valore t è chiamato traccia di Frobenius.

L'endomorfismo di Frobenius:

Su E(F_q), possiamo definire l'endomorfismo di Frobenius:

$\pi: E(\bar{F}_q) \to E(\bar{F}_q)$ $\pi(x, y) = (x^q, y^q)$

dove $\bar{F}_q$ è la chiusura algebrica di F_q.

Questo endomorfismo soddisfa un'equazione caratteristica:

$\pi^2 - [t]\pi + [q] = 0$

dove [n] denota la moltiplicazione per n nel gruppo E.

Teorema: I punti F_q-razionali di E sono esattamente i punti fissati da π:

$E(F_q) = \{P \in E(\bar{F}_q) : \pi(P) = P\}$

Dimostrazione: Un punto $(x, y) \in E$ è fissato da π se e solo se $x^q = x$ e $y^q = y$, cioè se e solo se $x, y \in F_q$. ∎

Punti su estensioni:

Per un'estensione $F_{(q^n)}$ di F_q, i punti $E(F_{(q^n)})$ sono i punti fissati da π^n:

$E(F_{(q^n)}) = \{P \in E(\bar{F}_q) : \pi^n(P) = P\}$

La struttura di $E(F_{(q^n)})$ come gruppo abeliano può essere completamente determinata dalla traccia t e dall'estensione n usando la teoria di Galois.

Teorema (Weil): Sia E(F_q) una curva ellittica con traccia di Frobenius t. Allora per ogni $n \geq 1$:

$|E(F_{(q^n)})| = q^n + 1 - (\alpha^n + \beta^n)$

dove α e β sono le radici del polinomio caratteristico:

$X^2 - tX + q = 0$

Esempio: Consideriamo la curva $y^2 = x^3 + x + 1$ su F_5.

Enumerando i punti:

- $x = 0$: $y^2 = 1$, quindi $y = \pm 1$ → punti (0,1), (0,4)
- $x = 1$: $y^2 = 3$, che non è un quadrato in F_5 → nessun punto
- $x = 2$: $y^2 = 11 \equiv 1 \pmod 5$, quindi $y = \pm 1$ → punti (2,1), (2,4)

- $x = 3$: $y^2 = 31 \equiv 1 \pmod 5$, quindi $y = \pm 1 \rightarrow$ punti (3,1), (3,4)
- $x = 4$: $y^2 = 69 \equiv 4 \pmod 5$, quindi $y = \pm 2 \rightarrow$ punti (4,2), (4,3)

Totale: 8 punti affini + punto all'infinito O = 9 punti.

Quindi $|E(F_5)| = 9 = 5 + 1 - (-3)$, quindi $t = -3$.

Per $F_{25} = F_{(5^2)}$:

$\alpha, \beta = (3 \pm \sqrt{(9 - 20)})/2 = (3 \pm \sqrt{(-11)})/2$

In F_{25}, $-11 \equiv 14$, e $\sqrt{14}$ esiste (perché $14^{((25-1)/2)} = 14^{12} \equiv 1 \pmod{25}$). Calcolando:

$|E(F_{25})| = 25 + 1 - (\alpha^2 + \beta^2) = 26 - ((\alpha+\beta)^2 - 2\alpha\beta) = 26 - (9 - 10) = 27$

6.4 Crittografia Basata su Accoppiamenti (Pairing-Based Cryptography)

Una delle applicazioni più sofisticate della teoria di Galois in crittografia riguarda gli accoppiamenti bilineari su curve ellittiche.

Accoppiamenti di Weil e Tate:

Sia E una curva ellittica su F_q e sia r un primo che divide $|E(F_q)|$. Il grado di immersione (embedding degree) k è il più piccolo intero positivo tale che r divide $q^k - 1$.

Un accoppiamento bilineare è una mappa:

$e: E[r] \times E[r] \rightarrow F^*_{(q^k)}$

dove E[r] denota i punti di r-torsione di E, che soddisfa:

1. **Bilinearità**: $e([a]P, [b]Q) = e(P, Q)^{(ab)}$
2. **Non-degeneratezza**: Se $e(P, Q) = 1$ per ogni Q, allora $P = O$
3. **Calcolabilità efficiente**: Esiste un algoritmo polinomiale per calcolare e(P, Q)

Il ruolo della teoria di Galois:

I punti di r-torsione E[r] possono non essere tutti definiti su F_q. In generale:

$E[r] \subseteq E(F_{(q^k)})$

La struttura galoisiana dell'estensione $F_{(q^k)}/F_q$ determina come i punti di r-torsione si distribuiscono.

Il gruppo di Galois $Gal(F_{(q^k)}/F_q) \cong Z/kZ$ agisce sui punti di E[r], e questa azione è cruciale per:

- Determinare quali accoppiamenti sono calcolabili efficientemente
- Comprendere la sicurezza dei protocolli basati su accoppiamenti
- Ottimizzare le implementazioni

Applicazioni crittografiche:

1. **Identity-Based Encryption (IBE)**: Lo schema di Boneh-Franklin usa accoppiamenti per permettere cifratura dove la chiave pubblica è semplicemente l'identità dell'utente (ad esempio, un indirizzo email).

2. **Short Signatures**: Lo schema BLS (Boneh-Lynn-Shacham) produce firme digitali molto compatte (circa 160 bit per 80 bit di sicurezza).

3. **Protocolli tripartiti one-round**: Tre parti possono stabilire una chiave condivisa con un solo scambio di messaggi, impossibile senza accoppiamenti.

Esempio concreto: Consideriamo E: $y^2 = x^3 + 2x + 3$ su $F_{(11^3)}$.

Questa curva ha embedding degree $k = 3$ per $r = 7$, quindi possiamo definire un accoppiamento:

$e: E[7] \times E[7] \to F^*_{(11^3)}$

Dove $F_{(11^3)} = F_{11}[x]/(x^3 + x + 4)$ è il campo con $11^3 = 1331$ elementi.

Il calcolo esplicito di un accoppiamento richiede l'algoritmo di Miller, che è basato sulla divisione di funzioni razionali sulla curva. La complessità computazionale è O(log r), dove r è l'ordine del sottogruppo, rendendolo pratico per curve opportunamente scelte.

Sicurezza degli accoppiamenti:

La sicurezza dei sistemi basati su accoppiamenti si basa sul problema del logaritmo discreto sia nel gruppo della curva ellittica E(F_q) che nel gruppo moltiplicativo F*_(q^k). La scelta del grado di immersione k è critica:

- Se k è troppo piccolo (ad esempio k = 1 o k = 2), il problema del logaritmo discreto in F*_(q^k) diventa troppo facile.
- Se k è troppo grande, il calcolo dell'accoppiamento diventa computazionalmente impraticabile.
- In pratica, si usano curve con k tra 6 e 12 per bilanciare sicurezza ed efficienza.

La teoria di Galois entra in gioco perché il grado di immersione k è essenzialmente l'ordine moltiplicativo di q modulo r, che è strettamente legato alla struttura del gruppo di Galois Gal(F_(q^k)/F_q).

6.5 Codici Correttori di Errori e Campi di Galois

I codici correttori di errori sono essenziali nelle comunicazioni digitali moderne, dalla trasmissione satellitare ai dischi rigidi, e sono profondamente radicati nella teoria dei campi finiti.

Codici di Reed-Solomon

I codici di Reed-Solomon sono tra i più importanti codici correttori e utilizzano direttamente l'aritmetica nei campi di Galois.

Definizione: Un codice di Reed-Solomon RS(n, k) su F_q è definito come segue:

- Messaggi: sequenze di k simboli da F_q, interpretate come coefficienti di un polinomio m(x) = m_0 + m_1 x + ... + m_(k-1) x^(k-1) di grado < k.
- Codifica: Si valuta m(x) in n punti distinti α_1, ..., α_n ∈ F_q, producendo la parola codice (m(α_1), m(α_2), ..., m(α_n)).

Proprietà fondamentali:

1. **Dimensione:** Il codice ha dimensione k (numero di simboli di informazione).
2. **Lunghezza:** Il codice ha lunghezza n (numero totale di simboli trasmessi).
3. **Distanza minima:** La distanza minima è d = n - k + 1.

Per il teorema di Singleton, questa è la massima distanza possibile per un codice di dimensione k e lunghezza n, rendendo i codici di Reed-Solomon codici MDS (Maximum Distance Separable).

Capacità di correzione: Un codice RS(n, k) può correggere fino a t = ⌊(n - k)/2⌋ errori di simbolo.

Dimostrazione della distanza minima:

Due polinomi distinti di grado < k possono coincidere in al massimo k - 1 punti. Quindi due parole codice distinte differiscono in almeno n - (k - 1) = n - k + 1 posizioni.

Decodifica:

Il processo di decodifica utilizza la struttura algebrica di F_q:

1. Si ricevono n simboli, alcuni potenzialmente errati.
2. Si cerca il polinomio di grado < k più vicino (nel senso della distanza di Hamming) ai valori ricevuti.
3. Gli algoritmi di decodifica, come l'algoritmo di Berlekamp-Welch o l'algoritmo di Gao, usano l'algebra polinomiale su F_q.

Esempio concreto in F_8:

Consideriamo RS(7, 3) su F_8 = F_(2^3) con polinomio irriducibile $x^3 + x + 1$.

Gli elementi di F_8 possono essere rappresentati come {0, 1, α, α^2, α^3, α^4, α^5, α^6} dove $\alpha^3 = \alpha + 1$.

Messaggio: (α^2, α, 1) rappresenta il polinomio $m(x) = \alpha^2 + \alpha x + x^2$.

Codifica: valutiamo m(x) nei punti 0, 1, α, α^2, α^3, α^4, α^5:

- $m(0) = \alpha^2$
- $m(1) = 1 + \alpha + \alpha^2 = \alpha^4$ (calcolando in F_8)

- $m(\alpha) = \alpha^2 + \alpha^2 + \alpha^2 = \alpha^2$
- $m(\alpha^2) = \alpha^2 + \alpha^3 + \alpha^4$
- ... (e così via)

La parola codice risultante è una sequenza di 7 simboli da F_8.

Applicazioni pratiche:

- **CD e DVD:** Usano codici RS per correggere graffi e imperfezioni.
- **Codici QR:** Implementano RS per robustezza contro danni parziali.
- **Comunicazioni spaziali:** Le missioni Voyager usano RS(255, 223) su F_256.
- **RAID 6:** I sistemi di storage usano RS per tollerare guasti multipli di dischi.

Teoria di Galois e Codici BCH

I codici BCH (Bose-Chaudhuri-Hocquenghem) sono una generalizzazione dei codici di Reed-Solomon che sfrutta profondamente la struttura delle estensioni di campi.

Definizione tramite radici:

Un codice BCH di lunghezza n su F_q con distanza progettata δ è definito come l'insieme di tutte le parole c = (c_0, c_1, ..., c_(n-1)) tali che il polinomio corrispondente:

c(x) = c_0 + c_1 x + ... + c_(n-1) x^(n-1)

ha come radici un insieme consecutivo di elementi β, β², β³, ..., β^(δ-1) dove β è una radice n-esima primitiva dell'unità in qualche estensione F_(q^m).

Il ruolo della teoria di Galois:

La chiave è che β potrebbe non appartenere a F_q, ma a un'estensione F_(q^m). Il gruppo di Galois Gal(F_(q^m)/F_q) agisce sulle radici, e questa azione determina la struttura del codice.

Polinomio generatore:

Il polinomio generatore g(x) di un codice BCH è il polinomio di grado minimo su F_q che ha β, β², ..., β^(δ-1) come radici:

g(x) = lcm(m_1(x), m_2(x), ..., m_(δ-1)(x))

dove m_i(x) è il polinomio minimo di β^i su F_q.

Connessione con la teoria di Galois:

Ogni β^i genera un'estensione semplice $F_q(\beta^i) \subseteq F_{(q^m)}$, e il polinomio minimo m_i(x) codifica le proprietà galoisiane di questa estensione. Le radici di m_i(x) sono esattamente i coniugati galoisiani di β^i:

radici(m_i(x)) = {β^i, β^(iq), β^(iq²), ..., β^(iq^(r-1))}

dove r = [F_q(β^i) : F_q] è il grado dell'estensione.

Esempio: Codice BCH binario di lunghezza 15.

Consideriamo F_16 = F_(2^4) con polinomio irriducibile $x^4 + x + 1$. Sia α una radice primitiva di ordine 15.

Per un codice BCH con distanza progettata δ = 5, dobbiamo trovare il polinomio che ha α, α^2, α^3, α^4 come radici.

I polinomi minimi su F_2 sono:

- m_1(x) = polinomio minimo di α: usando il fatto che i coniugati di α su F_2 sono α, α^2, α^4, α^8, otteniamo m_1(x) = $(x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8) = x^4 + x + 1$
- m_3(x) = polinomio minimo di α^3: i coniugati sono α^3, α^6, α^{12}, α^9, quindi m_3(x) = $(x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}) = x^4 + x^3 + x^2 + x + 1$

Il polinomio generatore è: g(x) = lcm(m_1(x), m_3(x)) = m_1(x) · m_3(x) = $(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^7 + x^6 + x^4 + 1$

Questo codice BCH(15, 7) ha 7 bit di informazione (perché 15 - 8 = 7) e può correggere fino a 2 errori.

Capitolo 7: Teoria di Kummer e Estensioni Cicliche

La teoria di Kummer fornisce una descrizione esplicita delle estensioni abeliane (e in particolare cicliche) di campi che contengono opportune radici dell'unità.

7.1 Radici dell'Unità

Definizione: Un elemento ζ in un campo K è una radice n-esima dell'unità se ζ^n = 1. È detta radice primitiva n-esima se ha ordine esattamente n, cioè se ζ^k ≠ 1 per 0 < k < n.

Proposizione: In un campo di caratteristica zero (o di caratteristica p con p non dividendo n), l'insieme μ_n delle radici n-esime dell'unità forma un gruppo ciclico di ordine n.

Dimostrazione:

Il polinomio x^n - 1 ha al massimo n radici in un campo. Il suo insieme di radici forma un sottogruppo del gruppo moltiplicativo K*, quindi è ciclico (perché ogni sottogruppo finito di K* è ciclico). Se ζ è una radice primitiva, allora μ_n = {1, ζ, ζ², ..., ζ^(n-1)} ≅ Z/nZ.

Polinomio ciclotomico:

Il polinomio ciclotomico Φ_n(x) è il polinomio monico i cui radici sono esattamente le radici primitive n-esime dell'unità:

Φ_n(x) = ∏_(gcd(k,n)=1, 1≤k≤n) (x - e^(2πik/n))

Questo polinomio ha grado φ(n) (funzione totiente di Eulero) ed è irriducibile su Q.

Formula di fattorizzazione:

$x^n - 1 = \prod_{d|n} \Phi_d(x)$

Esempi:

- $\Phi_1(x) = x - 1$
- $\Phi_2(x) = x + 1$
- $\Phi_3(x) = x^2 + x + 1$
- $\Phi_4(x) = x^2 + 1$
- $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$
- $\Phi_6(x) = x^2 - x + 1$
- $\Phi_8(x) = x^4 + 1$
- $\Phi_{12}(x) = x^4 - x^2 + 1$

7.2 Estensioni Ciclotomiche

Definizione: Il campo ciclotomico $Q(\zeta_n)$ è l'estensione di Q ottenuta aggiungendo una radice primitiva n-esima dell'unità ζ_n.

Teorema: Il gruppo di Galois di $Q(\zeta_n)/Q$ è isomorfo al gruppo delle unità $(Z/nZ)^*$:

$Gal(Q(\zeta_n)/Q) \cong (Z/nZ)^*$

Dimostrazione (schema):

Ogni $\sigma \in Gal(Q(\zeta_n)/Q)$ deve mappare ζ_n in un'altra radice primitiva n-esima, diciamo ζ_n^a dove $\gcd(a, n) = 1$. Definiamo:

$\varphi: Gal(Q(\zeta_n)/Q) \to (Z/nZ)^* \quad \sigma \mapsto a$ se $\sigma(\zeta_n) = \zeta_n^a$

Questa mappa è un isomorfismo di gruppi:

- È un omomorfismo: $(\sigma\tau)(\zeta_n) = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^b) = (\sigma(\zeta_n))^b = (\zeta_n^a)^b = \zeta_n^{(ab)}$
- È iniettivo: se $\sigma(\zeta_n) = \zeta_n$ allora σ fissa $Q(\zeta_n)$ (che è generato da ζ_n), quindi σ = id
- È suriettivo: per ogni a coprimo con n, possiamo definire $\sigma_a(\zeta_n) = \zeta_n^a$ e questo si estende a un automorfismo di $Q(\zeta_n)$

Esempio: $Q(\zeta_5)/Q$

Il polinomio minimo di $\zeta_5 = e^{(2\pi i/5)}$ è $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, quindi $[Q(\zeta_5):Q] = 4$.

Le radici primitive sono ζ_5, ζ_5^2, ζ_5^3, ζ_5^4, e il gruppo di Galois ha 4 elementi:

- $\sigma_1: \zeta_5 \mapsto \zeta_5$ (identità)
- $\sigma_2: \zeta_5 \mapsto \zeta_5^2$

- $\sigma_3: \zeta_5 \mapsto \zeta_5^3$
- $\sigma_4: \zeta_5 \mapsto \zeta_5^4$

Questo gruppo è isomorfo a $(Z/5Z)^* = \{1, 2, 3, 4\}$ con moltiplicazione modulo 5, che è ciclico di ordine 4 generato da 2.

7.3 Teoria di Kummer

La teoria di Kummer descrive esplicitamente le estensioni abeliane di esponente dividendo n quando il campo base contiene tutte le radici n-esime dell'unità.

Teorema di Kummer: Sia K un campo di caratteristica zero (o di caratteristica p con p non dividendo n) che contiene tutte le radici n-esime dell'unità, cioè $\mu_n \subseteq K$. Sia L/K un'estensione finita di grado dividendo n. Allora L/K è ciclica (cioè Gal(L/K) è ciclico) se e solo se $L = K(\alpha)$ dove $\alpha^n \in K$.

Dimostrazione ($\Rightarrow$):

Supponiamo L/K ciclica con $Gal(L/K) = \langle\sigma\rangle$ di ordine d dividendo n. Per la teoria dei caratteri, esiste $\alpha \in L$ tale che la norma $N_{(L/K)}(\alpha)$ genera K^*/K^{*n}. Possiamo mostrare che $\alpha^d \in K$ e $L = K(\alpha)$.

Dimostrazione ($\Leftarrow$):

Supponiamo $L = K(\alpha)$ con $a = \alpha^n \in K$. Ogni $\sigma \in Gal(L/K)$ mappa α in un'altra radice n-esima di a. Poiché K contiene tutte le radici n-esime dell'unità, tutte le radici n-esime di a hanno la forma $\zeta\alpha$ per qualche $\zeta \in \mu_n$.

Quindi $\sigma(\alpha) = \zeta_\sigma \alpha$ per qualche $\zeta_\sigma \in \mu_n$. Possiamo definire:

$\chi: Gal(L/K) \to \mu_n \ \sigma \mapsto \zeta_\sigma$

Questo è un omomorfismo iniettivo, quindi Gal(L/K) è isomorfo a un sottogruppo di μ_n, che è ciclico. Quindi Gal(L/K) è ciclico.

Generalizzazione (Estensioni abeliane di esponente n):

Il gruppo $K^*/(K^*)^n$ parametrizza le estensioni abeliane di K di esponente dividendo n:

Esiste una corrispondenza biunivoca tra:

- Sottogruppi di $K^*/(K^*)^n$
- Estensioni abeliane di K di esponente dividendo n contenute in una chiusura algebrica fissata

Questa corrispondenza è data da:

- $H \mapsto K(\{\alpha : \alpha^n \in H\})$
- $L \mapsto \{a \in K^* : x^n - a \text{ si spezza in } L\}/(K^*)^n$

7.4 Applicazioni Crittografiche della Teoria di Kummer

Le estensioni di Kummer appaiono naturalmente in diversi contesti crittografici.

Crittografia basata su accoppiamenti di Weil:

Nella costruzione di curve ellittiche con embedding degree prescritto, si cercano curve E su F_q tali che il sottogruppo di r-torsione E[r] abbia una struttura favorevole. Quando r divide q - 1, le estensioni di Kummer Q(ζ_r)/Q giocano un ruolo nella classificazione di tali curve.

Curve di Kummer per ECC:

Le curve di Kummer sono quozienti di curve ellittiche che permettono calcoli più efficienti per certi protocolli crittografici. Il loro gruppo di Galois ha una struttura che può essere sfruttata per ottimizzazioni.

Logaritmo discreto in campi finiti:

Gli algoritmi più avanzati per il logaritmo discreto in F_(q^n) utilizzano la struttura delle estensioni ciclotomiche e di Kummer per fattorizzare il problema in sottoproblemi più gestibili.

Capitolo 8: Applicazioni Avanzate in Crittografia

8.1 Diffie-Hellman e ElGamal su Campi Finiti

Il protocollo di scambio chiavi Diffie-Hellman e il cifrario ElGamal si basano sulla difficoltà del problema del logaritmo discreto in gruppi opportuni, tipicamente F*_p o gruppi di curve ellittiche.

Protocollo Diffie-Hellman:

1. Alice e Bob concordano pubblicamente su un primo p grande e un generatore g di F*_p (o di un sottogruppo di ordine primo q).
2. Alice sceglie casualmente a ∈ {1, ..., p-2} e calcola A = g^a mod p.
3. Bob sceglie casualmente b ∈ {1, ..., p-2} e calcola B = g^b mod p.
4. Alice e Bob si scambiano A e B pubblicamente.
5. Alice calcola K = B^a = g^(ab) mod p.
6. Bob calcola K = A^b = g^(ab) mod p.

La chiave condivisa K = g^(ab) può essere usata per cifratura simmetrica. Un attaccante che intercetta A e B dovrebbe risolvere il problema del logaritmo discreto per recuperare a o b.

Il ruolo della teoria di Galois:

La sicurezza di Diffie-Hellman dipende dalla struttura del gruppo F*_p. La teoria di Galois ci dice che:

F*_p ≅ Z/(p-1)Z

è ciclico, e questa struttura è essenziale per:

- Garantire l'esistenza di generatori
- Comprendere la distribuzione delle potenze
- Analizzare la complessità degli algoritmi di logaritmo discreto

Sottogruppi e sicurezza:

In pratica, si lavora spesso in un sottogruppo di ordine primo q di F*_p, dove q | (p-1). La fattorizzazione p - 1 = q · r è legata alla struttura dei sottocampi di F_p. Se p = 2q + 1 è un primo di Sophie Germain, il sottogruppo di ordine q ha proprietà di sicurezza ottimali.

Cifrario ElGamal:

Il cifrario ElGamal estende Diffie-Hellman alla cifratura asimmetrica:

KeyGen:

- Scegli primo p, generatore g, esponente privato x
- Calcola h = g^x mod p
- Chiave pubblica: (p, g, h)
- Chiave privata: x

Encrypt(m): (dove m ∈ F_p)

- Scegli y casuale
- Calcola c_1 = g^y mod p e c_2 = m · h^y mod p
- Cifrato: (c_1, c_2)

Decrypt(c_1, c_2):

- Calcola m = c_2 · (c_1^x)^(-1) mod p

La correttezza segue da: c_2 · (c_1^x)^(-1) = m · h^y · (g^y)^(-x) = m · g^(xy) · g^(-xy) = m.

8.2 Crittosistema di McEliece

Il crittosistema di McEliece è uno dei pochi sistemi post-quantistici pratici, basato sulla teoria dei codici correttori.

Costruzione:

KeyGen:

1. Scegli un codice binario di Goppa C di dimensione k e lunghezza n su F_(2^m), con capacità di correzione t errori.
2. Sia G una matrice generatrice k × n del codice in forma standard.
3. Scegli una matrice S invertibile k × k e una matrice di permutazione P (n × n).
4. Calcola G' = S · G · P.
5. Chiave pubblica: (G', t)

6. Chiave privata: (S, G, P)

Encrypt(m): (dove m è un vettore di k bit)

- Scegli un vettore di errore casuale e con peso di Hamming ≤ t
- Calcola c = m · G' ⊕ e
- Cifrato: c

Decrypt(c):

- Calcola c' = c · P^(-1) = m · S · G ⊕ e'
- Usa l'algoritmo di decodifica del codice di Goppa per recuperare m · S da c'
- Calcola m = (m · S) · S^(-1)

Il ruolo della teoria di Galois:

I codici di Goppa sono definiti tramite polinomi su F_(2^m). Un codice di Goppa è l'insieme delle parole c = (c_0, ..., c_(n-1)) tali che:

Σ_(i=0)^(n-1) c_i / (x - α_i) ≡ 0 (mod g(x))

dove α_0, ..., α_(n-1) sono elementi distinti di F_(2^m) e g(x) è un polinomio irriducibile su F_(2^m) di grado t.

La struttura di F_(2^m) come estensione di Galois di F_2 è cruciale per:

- Definire efficientemente i codici di Goppa
- Implementare gli algoritmi di decodifica
- Analizzare le proprietà di correzione

Il gruppo di Galois Gal(F_(2^m)/F_2) agisce sugli elementi α_i, e questa azione determina proprietà importanti del codice.

Sicurezza post-quantistica:

Mentre gli algoritmi quantistici di Shor possono risolvere il logaritmo discreto e la fattorizzazione, non esiste attualmente un algoritmo quantistico efficiente per il problema della decodifica di codici lineari generici, rendendo McEliece resistente agli attacchi quantistici.

8.3 Crittografia su Reticoli e Connessioni Galoisiane

La crittografia su reticoli è una delle aree più promettenti per la crittografia post-quantistica. Sorprendentemente, la teoria di Galois appare anche qui.

Reticoli ideali:

Un reticolo ideale è un reticolo che corrisponde a un ideale in un anello di interi algebrici. Sia K = Q(α) un campo numerico algebrico dove α è una radice di un polinomio irriducibile f(x) ∈ Z[x] di grado n.

L'anello di interi O_K di K può essere visto come un reticolo in R^n. Gli ideali di O_K forniscono sottoreticoli con proprietà algebriche ricche.

Ring-LWE (Ring Learning With Errors):

Il problema Ring-LWE lavora nell'anello R = Z[x]/(f(x)) dove f(x) è un polinomio ciclotomico (tipicamente f(x) = x^n + 1 con n potenza di 2).

Gli elementi di R possono essere visti come polinomi di grado < n con coefficienti interi, e la moltiplicazione è modulo f(x).

Il ruolo della teoria di Galois:

L'anello R = Z[x]/(x^n + 1) è strettamente legato al campo ciclotomico Q(ζ_(2n)) dove ζ_(2n) è una radice 2n-esima primitiva dell'unità.

Il gruppo di Galois Gal(Q(ζ_(2n))/Q) ≅ (Z/2nZ)* agisce su R in modo naturale, e questa azione ha importanti conseguenze:

1. **Attacchi basati su sottocampi:** Se l'azione di Galois non è "mescolata" abbastanza, un attaccante potrebbe sfruttare la struttura dei sottocampi per attacchi più efficienti.

2. **Riduzione di sicurezza:** La dimostrazione che Ring-LWE è difficile si basa su riduzioni worst-case to average-case che usano la teoria algebrica dei numeri e, indirettamente, la teoria di Galois.

3. **Scelta del campo numerico:** La sicurezza di Ring-LWE dipende dalla scelta di f(x). I polinomi ciclotomici sono preferiti perché permettono implementazioni FFT efficienti, ma la loro struttura galoisiana deve essere considerata attentamente.

NTRU (N-th degree TRUncated polynomial ring):

NTRU è un altro crittosistema basato su reticoli ideali che precede Ring-LWE.

KeyGen:

- Scegli parametri n (primo), p, q (coprimi, tipicamente p piccolo e q grande)
- Lavora nell'anello R = Z[x]/(x^n - 1)
- Scegli polinomi piccoli f, g ∈ R con f invertibile modulo p e modulo q
- Calcola h = g · f^(-1) mod q
- Chiave pubblica: h
- Chiave privata: (f, g)

Encrypt(m): (dove m ∈ R con coefficienti piccoli)

- Scegli un polinomio piccolo casuale r
- Calcola c = p · r · h + m mod q
- Cifrato: c

Decrypt(c):

- Calcola a = f · c mod q (riducendo i coefficienti nell'intervallo (-q/2, q/2])
- Calcola m = a mod p

La correttezza e sicurezza di NTRU dipendono dalla difficoltà di trovare vettori corti in reticoli, ma anche dalla struttura dell'anello R = Z[x]/(x^n - 1), che ha connessioni con i campi ciclotomici quando n è primo.

Capitolo 9: Teoria di Galois Differenziale

Una generalizzazione profonda della teoria di Galois classica si applica alle equazioni differenziali, con sorprendenti applicazioni in fisica teorica e teoria del controllo.

9.1 Estensioni Differenziali

Definizione: Un campo differenziale è una coppia (K, ∂) dove K è un campo e ∂: K → K è una derivazione, cioè un'applicazione che soddisfa:

- $\partial(a + b) = \partial(a) + \partial(b)$
- $\partial(ab) = a\partial(b) + b\partial(a)$ (regola di Leibniz)

Il campo delle costanti è C_K = {a ∈ K : ∂(a) = 0}.

Esempio: Il campo K = C(x) delle funzioni razionali in x con la derivazione standard ∂ = d/dx ha campo delle costanti C_K = C.

Definizione: Sia (K, ∂) un campo differenziale. Un'estensione differenziale è un campo differenziale (L, ∂') tale che K ⊆ L e ∂' estende ∂ (cioè $\partial'|_K = \partial$).

Esempio fondamentale: Consideriamo l'equazione differenziale y' = y. Una soluzione è y = e^x. L'estensione K(e^x)/K dove K = C(x) è un'estensione differenziale con ∂(e^x) = e^x.

9.2 Gruppo di Galois Differenziale

Gruppo di Galois Differenziale:

Analogamente alla teoria classica, possiamo definire il gruppo di Galois differenziale di un'estensione differenziale.

Definizione: Sia L/K un'estensione differenziale. Un automorfismo differenziale di L/K è un K-automorfismo σ: L → L che commuta con la derivazione, cioè σ(∂(a)) = ∂(σ(a)) per ogni a ∈ L.

Il gruppo di Galois differenziale Gal^∂(L/K) è il gruppo di tutti gli automorfismi differenziali di L/K.

Teorema di Picard-Vessiot:

Per equazioni differenziali lineari omogenee a coefficienti in K, esiste un'estensione minimale L/K (chiamata estensione di Picard-Vessiot) tale che:

1. L contiene un insieme fondamentale di soluzioni dell'equazione
2. L è generato su K da queste soluzioni e dalle loro derivate
3. Il campo delle costanti di L è uguale al campo delle costanti di K

Il gruppo di Galois differenziale Gal^∂(L/K) è un gruppo algebrico lineare (cioè un sottogruppo chiuso di GL_n(C) definito da equazioni polinomiali).

Esempio: Consideriamo l'equazione y'' - y = 0 su K = C(x).

Le soluzioni formano uno spazio vettoriale bidimensionale generato da e^x e e^(-x). L'estensione di Picard-Vessiot è L = K(e^x, e^(-x)).

Ogni automorfismo differenziale deve mappare e^x in c_1 e^x + c_2 e^(-x) per qualche costante c. Ma poiché ∂(e^x) = e^x, abbiamo:

∂(σ(e^x)) = σ(∂(e^x)) = σ(e^x)

Quindi c_1 e^x + c_2 e^(-x) deve soddisfare (c_1 e^x + c_2 e^(-x))' = c_1 e^x + c_2 e^(-x), da cui c_2 = 0 e σ(e^x) = c_1 e^x.

Analogamente σ(e^(-x)) = c_2' e^(-x). Il gruppo di Galois differenziale è quindi:

Gal^∂(L/K) ≅ {(c_1, c_2) : c_1, c_2 ∈ C*} ≅ (C*)² ≅ GL_2(C) ∩ {matrici diagonali}

9.3 Risolubilità di Equazioni Differenziali

Analogamente al caso algebrico, possiamo chiederci quando un'equazione differenziale è risolubile per quadrature (cioè usando integrali, esponenziali, e composizioni finite).

Teorema (Liouville): Un'equazione differenziale lineare è risolubile per quadrature se e solo se il suo gruppo di Galois differenziale è risolubile (come gruppo algebrico).

Questo è l'analogo differenziale del teorema di Galois sulla risolubilità per radicali!

Esempio: L'equazione di Bessel:

x² y'' + x y' + (x² - ν²) y = 0

Non è risolubile per quadrature in generale, perché il suo gruppo di Galois differenziale è SL_2(C), che non è risolubile per ν generico.

9.4 Applicazioni in Fisica Teorica

La teoria di Galois differenziale ha applicazioni profonde in fisica matematica.

Integrabilità di sistemi Hamiltoniani:

Un sistema Hamiltoniano è detto integrabile (nel senso di Liouville) se possiede un numero sufficiente di integrali primi in involuzione. La teoria di Galois differenziale fornisce criteri per determinare quando un sistema è non integrabile.

Teorema (Ziglin, Ramis, Morales-Ruiz): Se un sistema Hamiltoniano ha una variazione normale lungo una soluzione particolare con gruppo di Galois differenziale non virtualmente abeliano, allora il sistema non è integrabile (nel senso che non esistono integrali primi meromorfi sufficienti).

Esempio: Il problema dei tre corpi in meccanica celeste è stato dimostrato non integrabile usando questi metodi galoisiani.

Equazioni della fisica matematica:

Molte equazioni importanti in fisica hanno interpretazioni galoisiane:

1. **Equazione di Schrödinger:** Le soluzioni dell'equazione di Schrödinger per un potenziale dato formano un'estensione differenziale, e il gruppo di Galois differenziale codifica le simmetrie quantistiche del sistema.

2. **Equazioni di Yang-Mills:** Le connessioni gauge possono essere studiate usando generalizzazioni della teoria di Galois differenziale.

3. **Equazioni isomonodromatiche:** Equazioni come Painlevé hanno gruppi di monodromia che sono strettamente legati ai gruppi di Galois differenziali.

Capitolo 10: Generalizzazioni e Teorie Avanzate

10.1 Teoria di Galois Infinita

Fino ad ora ci siamo concentrati su estensioni finite, ma molte estensioni importanti sono infinite.

Definizione: Sia L/K un'estensione algebrica (possibilmente infinita). Il gruppo di Galois Gal(L/K) è il gruppo di tutti i K-automorfismi di L, dotato della topologia di Krull:

Una base di intorni dell'identità è data dai sottogruppi Gal(L/E) dove E varia su tutti i campi intermedi finiti $K \subseteq E \subseteq L$.

Con questa topologia, Gal(L/K) diventa un gruppo topologico compatto totalmente disconnesso (un gruppo profinito).

Teorema Fondamentale della Teoria di Galois Infinita:

Sia L/K un'estensione di Galois (possibilmente infinita, ma con L chiusura algebrica di K se vogliamo il massimo di generalità). Allora esiste una corrispondenza biunivoca tra:

{sottogruppi chiusi H di Gal(L/K)} $\leftrightarrow$ {campi intermedi $K \subseteq E \subseteq L$}

data da H ↦ L^H e E ↦ Gal(L/E).

Questa corrispondenza inverte le inclusioni e preserva la normalità.

Esempio fondamentale: La chiusura algebrica $\bar{Q}$ di Q.

Il gruppo Gal($\bar{Q}$/Q) è un gruppo profinito estremamente complicato, chiamato gruppo di Galois assoluto di Q. La sua struttura codifica profonde informazioni aritmetiche sui numeri algebrici.

Ogni campo numerico finito K/Q corrisponde a un quoziente finito Gal(K/Q) ≅ Gal($\bar{Q}$/Q)/Gal($\bar{Q}$/K).

Estensioni abeliane e teoria dei campi di classe:

Un caso particolare importante è lo studio delle estensioni abeliane di un campo numerico. Il teorema di Kronecker-Weber afferma che:

Ogni estensione abeliana finita di Q è contenuta in un campo ciclotomico Q(ζ_n) per qualche n.

La teoria dei campi di classe generalizza questo a campi numerici arbitrari, fornendo una descrizione del gruppo di Galois abeliano massimale usando il gruppo di classi di ideali del campo base.

10.2 Cohomologia di Galois

La cohomologia di Galois è uno strumento potente per studiare le estensioni di campi e i gruppi di Galois.

Definizione: Sia L/K un'estensione di Galois con G = Gal(L/K). Per ogni G-modulo M (cioè un gruppo abeliano con un'azione di G), possiamo definire i gruppi di cohomologia di Galois:

$H^0(G, M) = M^G = \{m \in M : \sigma(m) = m \text{ per ogni } \sigma \in G\}$ $H^1(G, M) = \{1\text{-cocicli}\}/\{1\text{-cobordi}\}$ $H^2(G, M) = \{2\text{-cocicli}\}/\{2\text{-cobordi}\}$

dove i cocicli sono applicazioni che soddisfano certe condizioni di compatibilità, e i cobordi sono cocicli banali.

Teorema 90 di Hilbert:

Sia L/K un'estensione di Galois finita con G = Gal(L/K). Allora:

$H^1(G, L^*) = 0$

cioè ogni 1-cociclo a valori in L* è un cobordo.

Dimostrazione: Sia f: G → L* un 1-cociclo, cioè $f(\sigma\tau) = f(\sigma) \cdot \sigma(f(\tau))$ per ogni σ, τ ∈ G.

Per l'indipendenza lineare dei caratteri, esiste α ∈ L tale che $\beta = \Sigma_{(\sigma \in G)} f(\sigma)\, \sigma(\alpha) \neq 0$.

Per ogni $\tau \in G$: $\tau(\beta) = \Sigma_{(\sigma \in G)} \tau(f(\sigma)) \tau\sigma(\alpha) = \Sigma_{(\sigma \in G)} f(\tau)^{(-1)} f(\tau\sigma) \tau\sigma(\alpha) = f(\tau)^{(-1)} \Sigma_{(\rho \in G)} f(\rho) \rho(\alpha) = f(\tau)^{(-1)} \beta$

Quindi $f(\tau) = \beta/\tau(\beta)$, il che mostra che f è un cobordo (la derivata moltiplicativa di β).

Applicazioni:

1. **Algebre di divisione:** $H^2(G, L^*)$ classifica le algebre di divisione centrali su K con gruppo di Galois G (teorema di Brauer).

2. **Estensioni di gruppi:** La cohomologia di Galois appare nella teoria delle estensioni di gruppi e nello studio dei gruppi fondamentali in geometria algebrica.

3. **Forme quadratiche:** La cohomologia galoisiana è fondamentale nello studio delle forme quadratiche su campi arbitrari.

10.3 Teoria di Galois in Geometria Algebrica

La teoria di Galois ha profonde generalizzazioni geometriche che sono centrali nella matematica moderna.

Rivestimenti finiti:

In topologia algebrica, un rivestimento finito $X \to Y$ di spazi topologici connessi e localmente connessi per archi corrisponde a un'azione del gruppo fondamentale $\pi_1(Y)$ sull'insieme delle fibre.

Questa corrispondenza è un analogo topologico della corrispondenza di Galois.

Teoria di Galois per schemi:

In geometria algebrica, possiamo definire rivestimenti finiti étale di schemi, che generalizzano le estensioni finite separabili di campi.

Per uno schema connesso X, il gruppo fondamentale étale $\pi_1^{ét}(X)$ classifica i rivestimenti finiti étale di X, proprio come $Gal(\bar{K}/K)$ classifica le estensioni finite separabili di un campo K.

Teorema: Per un campo K, abbiamo:

$\pi_1^{ét}(\text{Spec } K) \cong Gal(\bar{K}/K)$

Questa identificazione permette di applicare tecniche geometriche allo studio dei gruppi di Galois, e viceversa.

Congettura di Grothendieck:

Grothendieck congetturò (e fu in gran parte dimostrata da Belyi e altri) una profonda connessione tra:

- Il gruppo di Galois assoluto $Gal(\bar{Q}/Q)$
- La teoria dei dessins d'enfants (grafi su superfici di Riemann)
- La geometria delle curve algebriche su campi numerici

Questa connessione ha portato a nuove prospettive sulla teoria dei numeri e sulla geometria algebrica.

10.4 Teoria di Galois Motivica

Una generalizzazione ancora più astratta è la teoria di Galois motivica, sviluppata da Grothendieck e continuata da molti matematici.

Idea di base:

Così come il gruppo di Galois classico $Gal(\bar{K}/K)$ agisce sulle estensioni algebriche, il gruppo di Galois motivico agisce su oggetti cohomologici più generali (motivi) associati a varietà algebriche.

Periodi e gruppo di Galois motivico:

I numeri periodici (come π, $\log 2$, valori speciali di funzioni L) possono essere studiati usando il gruppo di Galois motivico. Congetture profonde, come le congetture di periodi di Grothendieck, predicono relazioni tra periodi usando l'azione galoisiana.

Connessione con la fisica:

Sorprendentemente, il gruppo di Galois motivico appare nello studio delle ampiezze di Feynman nella teoria quantistica dei campi, suggerendo profonde connessioni tra teoria dei numeri, geometria algebrica e fisica delle particelle.

Capitolo 11: Applicazioni Computazionali e Implementazioni

11.1 Algoritmi per il Calcolo dei Gruppi di Galois

Il calcolo esplicito del gruppo di Galois di un polinomio è un problema computazionale importante con applicazioni in teoria dei numeri algoritmici e sistemi algebrici computerizzati.

Problema: Dato $p(x) \in Q[x]$ irriducibile di grado n, determinare $Gal(L/Q)$ dove L è il campo di spezzamento di p(x).

Approccio classico (Stauduhar):

1. Calcola il discriminante disc(p) e determina se è un quadrato perfetto (questo distingue tra S_n e A_n).
2. Calcola le risolventi di Lagrange per determinare sottogruppi.
3. Usa informazioni sulla fattorizzazione di p(x) modulo primi diversi.

Teorema di Frobenius:

La fattorizzazione di p(x) modulo un primo p (che non divide il discriminante) fornisce informazioni sulla struttura ciclica del gruppo di Galois.

Se p(x) ≡ p_1(x)^(e_1) · ... · p_r(x)^(e_r) (mod p) con p_i irriducibili di grado d_i, allora Gal(L/Q) contiene una permutazione di tipo ciclo (d_1, d_2, ..., d_r).

Esempio: Consideriamo $p(x) = x^5 - 2 \in Q[x]$.

Fattorizzazioni modulo vari primi:

- mod 3: $x^5 - 2 \equiv x^5 + 1 = (x + 1)(x^4 + 2x^3 + x^2 + 2x + 1)$ (grado 1 e 4)
- mod 7: irriducibile (grado 5)
- mod 11: si fattorizza in prodotto di irriducibili di gradi specifici

Queste informazioni, combinate con il fatto che deg(p) = 5 è primo e che p(x) ha esattamente 2 radici reali (usando il teorema di Descartes), permettono di concludere che Gal(L/Q) ≅ S_5.

Algoritmi moderni:

Software come Magma, Sage, e GAP implementano algoritmi sofisticati che combinano:

- Teoria della rappresentazione
- Calcolo con approssimazioni numeriche delle radici
- Tecniche p-adiche
- Algoritmi LLL per trovare relazioni

11.2 Implementazione di Aritmetica in Campi Finiti

L'implementazione efficiente di operazioni in F_(q^n) è cruciale per applicazioni crittografiche.

Scelta della rappresentazione:

1. **Rappresentazione polinomiale:** Elementi come polinomi di grado < n con coefficienti in F_q, modulo un polinomio irriducibile.
    - Vantaggio: Flessibile, funziona per ogni q e n
    - Svantaggio: Moltiplicazione richiede riduzione modulare
2. **Rappresentazione normale:** Usando una base normale {β, β^q, β^(q²), ..., β^(q^(n-1))} dove β è un elemento normale (cioè i suoi coniugati di Frobenius sono linearmente indipendenti).
    - Vantaggio: Elevamento al quadrato (applicazione di Frobenius) è solo una rotazione ciclica
    - Svantaggio: Moltiplicazione più complessa

3. **Rappresentazione tower:** Per n composto, rappresentare F_(q^n) come estensione di F_(q^m) dove m | n.

    - Vantaggio: Può ridurre la complessità computazionale sfruttando la struttura a torre
    - Svantaggio: Non sempre disponibile (richiede n composto)

Ottimizzazioni hardware:

Per F_(2^n) (caso binario), le operazioni possono essere implementate molto efficientemente:

Addizione: XOR bit a bit (una singola istruzione CPU)

Moltiplicazione: Algoritmi specializzati:

- Karatsuba per dimensioni medie (n ≈ 10-100)
- Toom-Cook per dimensioni maggiori
- FFT su campi finiti per dimensioni molto grandi (n > 1000)

Inversione:

- Metodo 1: Euclideo esteso O(n²) operazioni
- Metodo 2: Fermat (a^(-1) = a^(q^n - 2)) usando square-and-multiply O(n³) operazioni ma parallelizzabile
- Metodo 3: Tabelle precalcolate per campi piccoli

Esempio di implementazione (pseudocodice) per F_(2^8) nell'AES:

```
// Polinomio irriducibile: x^8 + x^4 + x^3 + x + 1 = 0x11B
const IRREDUCIBLE_POLY = 0x11B

function gf256_multiply(a, b):
    product = 0
    for i from 0 to 7:
        if (b & 1) != 0:
            product ^= a

        // Check se il bit alto di a è 1
        high_bit_set = (a & 0x80) != 0

        // Shift a sinistra
        a = (a << 1) & 0xFF

        // Se il bit alto era 1, riduci modulo polinomio irriducibile
        if high_bit_set:
            a ^= IRREDUCIBLE_POLY

        b >>= 1
```

```
    return product

function gf256_inverse(a):
    if a == 0:
        return 0
    // Usa a^254 = a^(-1) in F_256
    result = a
    for i from 1 to 6:
        result = gf256_multiply(result, result) // Quadrato
        result = gf256_multiply(result, a)      // Moltiplica per a
    result = gf256_multiply(result, result) // Ultimo quadrato
    return result
```

11.3 Librerie Crittografiche e Standard

Librerie principali:

1. **OpenSSL/LibreSSL:** Implementa AES, curve ellittiche, Diffie-Hellman
2. **libgcrypt:** Usata da GnuPG, implementa molti algoritmi basati su F_q
3. **Crypto++:** Libreria C++ con implementazioni ottimizzate
4. **NaCl/libsodium:** Focus su semplicità e sicurezza, usa Curve25519
5. **MIRACL:** Specializzata in aritmetica su curve ellittiche

Standard crittografici:

- **NIST FIPS 197:** Standard per AES
- **NIST FIPS 186-4:** Standard per firme digitali (DSA, ECDSA)
- **IEEE P1363:** Standard per crittografia a chiave pubblica
- **IETF RFC 5639:** Curve ellittiche Brainpool
- **NIST Post-Quantum Standards:** Nuovi standard per crittografia resistente ai computer quantistici

11.4 Timing Attacks e Implementazioni Sicure

Le implementazioni crittografiche devono difendersi da attacchi che sfruttano tempi di esecuzione variabili.

Problema: Se il tempo di calcolo dipende da bit della chiave segreta, un attaccante che misura i tempi può recuperare la chiave.

Esempio vulnerabile:

```
function insecure_multiply(a, b, secret_key):
    result = 0
    for each bit of secret_key:
        if bit == 1:
            result = add(result, a)  // Tempo variabile!
```

```
    a = double(a)
  return result
```

Contromisure:

1. **Operazioni a tempo costante:** Ogni branch deve prendere lo stesso tempo
2. **Mascheramento (masking):** Randomizzare valori intermedi
3. **Addizioni/moltiplicazioni sempre eseguite:** Non saltare operazioni in base a bit segreti

Implementazione sicura:

```
function secure_multiply(a, b, secret_key):
  result = 0
  for each bit of secret_key:
    // Sempre esegui entrambe le operazioni
    temp1 = add(result, a)
    temp2 = result

    // Selezione a tempo costante
    result = constant_time_select(bit, temp1, temp2)
    a = double(a)
  return result
```

La funzione `constant_time_select` deve essere implementata senza branch condizionali, tipicamente usando operazioni bitwise:

```
function constant_time_select(condition, value_if_true, value_if_false):
  // condition è 0 o 1
  mask = -condition  // 0x00...00 o 0xFF...FF
  return (mask & value_if_true) | (~mask & value_if_false)
```

Capitolo 12: Frontiere della Ricerca e Problemi Aperti

12.1 Problema Inverso di Galois

Enunciato: Per ogni gruppo finito G, esiste un'estensione di Galois L/Q tale che Gal(L/Q) ≅ G?

Questo problema, formulato nel XIX secolo, rimane uno dei grandi problemi aperti della teoria di Galois.

Risultati noti:

1. **Gruppi risolubili:** Shafarevich (1954) dimostrò che ogni gruppo finito risolubile è gruppo di Galois su Q.

2. **Gruppi simmetrici e alterni:** S_n e A_n sono gruppi di Galois su Q per ogni n (Hilbert lo sapeva già).

3. **Gruppi sporadici:** Molti dei 26 gruppi sporadici sono stati realizzati come gruppi di Galois, ma non tutti.

4. **Gruppi finiti semplici:** La maggior parte dei gruppi semplici finiti sono stati realizzati, grazie al lavoro di Thompson, Malle, e altri.

Approcci:

- **Metodo rigido:** Costruire polinomi con gruppo di Galois prescritto usando la teoria delle funzioni algebriche e i rivestimenti di Riemann.
- **Metodo costruttivo:** Usare embedding problems e teoria cohomologica.
- **Metodi computazionali:** Ricerca sistematica di polinomi con software algebrico.

12.2 Crittografia Post-Quantistica

Con l'avvento dei computer quantistici, molti sistemi crittografici basati su logaritmo discreto e fattorizzazione diventeranno insicuri. La teoria di Galois continua a giocare un ruolo nei nuovi sistemi post-quantistici.

Candidati principali:

1. **Crittografia su reticoli:** Come Ring-LWE, NTRU
    - Connessione: Usa anelli di interi in campi numerici, strutture galoisiane
2. **Crittografia basata su codici:** Come McEliece
    - Connessione: Usa codici su F_(2^m), teoria dei campi finiti
3. **Crittografia basata su hash:** Firme basate su funzioni hash
    - Connessione minima con Galois, ma spesso usano aritmetica in campi finiti
4. **Crittografia basata su isogenie:** Usa isogenie tra curve ellittiche
    - Connessione: Profondamente legata alla teoria di Galois delle curve ellittiche

NIST Post-Quantum Competition:

Nel 2022, NIST ha selezionato i primi standard:

- **CRYSTALS-Kyber:** Key encapsulation basato su Module-LWE
- **CRYSTALS-Dilithium:** Firma digitale basata su lattices
- **FALCON:** Firma digitale basata su lattices (NTRU)
- **SPHINCS+:** Firma basata su hash

Tutti eccetto SPHINCS+ hanno profonde connessioni con la teoria di Galois attraverso gli anelli ciclotomici e i campi finiti.

12.3 Relazioni con la Teoria dei Numeri Analitica

La teoria di Galois si intreccia profondamente con la teoria analitica dei numeri attraverso le funzioni L e le rappresentazioni galoisiane.

Funzioni L:

Per un'estensione galoisiana L/K, possiamo definire la funzione zeta di Dedekind:

ζ_L(s) = Σ_(ideali a di O_L) 1/(N(a)^s)

che si fattorizza come:

ζ_L(s) = Π_(χ: Gal(L/K) → C*) L(s, χ)

dove il prodotto è su tutti i caratteri del gruppo di Galois.

Congettura di Artin:

Per ogni carattere non banale irriducibile χ di Gal(L/K), la funzione L di Artin L(s, χ) ha un prolungamento analitico a tutto C e soddisfa un'equazione funzionale.

Questa congettura è stata dimostrata solo in casi speciali ed è uno dei grandi problemi aperti.

Programma di Langlands:

Il programma di Langlands, una delle più vaste congetture in matematica, predice profonde corrispondenze tra:

- Rappresentazioni galoisiane (teoria di Galois)
- Forme automorfe (analisi armonica)
- Rappresentazioni di gruppi algebrici

Queste connessioni hanno portato a risultati straordinari, inclusa la dimostrazione dell'ultimo teorema di Fermat da parte di Andrew Wiles.

12.4 Aspetti Computazionali del Programma di Langlands

Verificare numericamente le corrispondenze di Langlands richiede calcoli sofisticati con gruppi di Galois, forme modulari, e rappresentazioni.

LMFDB (L-functions and Modular Forms Database):

Un database online che cataloga:

- Campi numerici e i loro gruppi di Galois

- Curve ellittiche e le loro funzioni L
- Forme modulari
- Rappresentazioni galoisiane

Questo progetto usa algoritmi avanzati per calcolare gruppi di Galois di estensioni di grado fino a 23, esplorando regioni della matematica che erano inaccessibili teoricamente.

Conclusione: L'Eredità e il Futuro della Teoria di Galois

La teoria di Galois rappresenta uno dei trionfi più straordinari del pensiero matematico. Da un problema apparentemente concreto sulla risoluzione di equazioni polinomiali, Évariste Galois estrasse una teoria di portata universale che collega algebra, geometria, topologia, teoria dei numeri, e persino fisica teorica.

L'impatto storico:

La teoria di Galois ha rivoluzionato l'algebra moderna, introducendo il concetto di gruppo come strumento unificante e dimostrando il potere del pensiero strutturale. Ha mostrato che le proprietà di un oggetto matematico (un'estensione di campi) possono essere completamente codificate nelle simmetrie di quell'oggetto (il gruppo di Galois).

Le applicazioni pratiche:

Dalla crittografia moderna alla correzione di errori, dalla teoria dell'informazione alla progettazione di circuiti integrati, la teoria di Galois e le strutture algebriche che ha rivelato sono alla base di innumerevoli tecnologie contemporanee. Ogni volta che usiamo uno smartphone, accediamo a un sito web sicuro, o ascoltiamo musica da un CD, beneficiamo dell'aritmetica nei campi di Galois.

Le direzioni future:

La ricerca contemporanea continua a espandere le frontiere della teoria di Galois in direzioni che Galois stesso non avrebbe potuto immaginare:

- La teoria di Galois motivica di Grothendieck promette di unificare vaste aree della matematica
- Le connessioni con la fisica teorica attraverso le teorie gauge e la teoria delle stringhe continuano a sorprendere
- La crittografia post-quantistica basata su strutture galoisiane potrebbe proteggere la nostra sicurezza digitale nell'era quantistica
- I calcoli numerici e algoritmici stanno aprendo nuove finestre su strutture galoisiane che erano considerate irraggiungibili

Riflessioni filosofiche:

La teoria di Galois incarna una delle intuizioni più profonde della matematica: le simmetrie di un problema contengono la chiave per la sua soluzione. Questo principio, che Galois applicò alle equazioni algebriche, si è rivelato di portata universale, apparendo in fisica (dove le simmetrie determinano le leggi di conservazione), in chimica (dove le simmetrie molecolari

determinano proprietà fisiche), e in informatica (dove le simmetrie algoritmiche determinano la complessità).

La notte prima del suo fatale duello, Galois scrisse freneticamente le sue idee matematiche, consapevole che il tempo gli stava per scadere. In quelle pagine febbrili, un giovane di vent'anni gettò le basi di una teoria che avrebbe cambiato per sempre il corso della matematica. È una testimonianza della potenza delle idee matematiche che, quasi due secoli dopo, le intuizioni di Galois non solo sopravvivono ma continuano a generare nuova matematica e nuove applicazioni.

La storia della teoria di Galois è anche una storia umana di tragedia e trionfo. Galois morì prima di vedere la sua teoria compresa e apprezzata. I suoi lavori furono inizialmente respinti dall'establishment matematico, che non riusciva a comprendere la radicalità delle sue idee. Ci vollero decenni prima che matematici come Camille Jordan e Leopold Kronecker riconoscessero il genio di Galois e sviluppassero la sua teoria nella forma che conosciamo oggi.

Appendice A: Complementi Tecnici e Dimostrazioni

A.1 Dimostrazione Completa dell'Irriducibilità di $x^4 - 2$

Dimostriamo che $p(x) = x^4 - 2$ è irriducibile su Q usando il criterio di Eisenstein.

Criterio di Eisenstein: Sia p(x) = a_n x^n + a_(n-1) x^(n-1) + ... + a_1 x + a_0 ∈ Z[x]. Se esiste un primo p tale che:

1. p divide a_i per ogni i < n
2. p non divide a_n
3. p^2 non divide a_0

allora p(x) è irriducibile su Q.

Applicazione: Per $p(x) = x^4 - 2$, scegliamo il primo p = 2:

1. 2 divide -2 (il termine costante) ✓
2. 2 non divide 1 (il coefficiente di x^4) ✓
3. $4 = 2^2$ non divide -2 ✓

Quindi $x^4 - 2$ è irriducibile su Q.

Significato: Questo significa che $\sqrt[4]{2}$ ha polinomio minimo di grado 4 su Q, quindi $[Q(\sqrt[4]{2}):Q] = 4$.

A.2 Struttura Esplicita del Gruppo Diedrale D_4

Il gruppo diedrale D_4 (simmetrie del quadrato) ha 8 elementi e può essere presentato come:

D_4 = ⟨r, s | $r^4 = s^2 = 1$, srs = r^(-1)⟩

dove r rappresenta una rotazione di 90° e s una riflessione.

Elementi:

- e (identità)
- r (rotazione 90°)
- r^2 (rotazione 180°)
- r^3 (rotazione 270°)
- s (riflessione rispetto asse verticale)
- sr (riflessione rispetto diagonale)
- sr^2 (riflessione rispetto asse orizzontale)
- sr^3 (riflessione rispetto altra diagonale)

Tavola di moltiplicazione:

	e	**r**	**r^2**	**r^3**	**s**	**sr**	**sr^2**	**sr^3**
e	e	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	e	sr^3	s	sr	sr^2
r^2	r^2	r^3	e	r	sr^2	sr^3	s	sr
r^3	r^3	e	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	e	r	r^2	r^3
sr	sr	sr^2	sr^3	s	r^3	e	r	r^2
sr^2	sr^2	sr^3	s	sr	r^2	r^3	e	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	e

Sottogruppi normali:

1. {e} (banale)
2. {e, r^2} (centro di D_4)
3. {e, r, r^2, r^3} (rotazioni, isomorfo a Z/4Z)
4. D_4 (totale)

Quozienti:

- D_4/{e} ≅ D_4
- D_4/{e, r^2} ≅ Z/2Z × Z/2Z
- D_4/{e, r, r^2, r^3} ≅ Z/2Z
- D_4/D_4 ≅ {e}

A.3 Calcolo Esplicito nel Campo GF(2^8)

Eseguiamo alcuni calcoli dettagliati in GF(2^8) con il polinomio irriducibile dell'AES: $m(x) = x^8 + x^4 + x^3 + x + 1$.

Esempio 1: Moltiplicazione di 53_{16} e CA_{16}

$53_{16} = 01010011_2 = x^6 + x^4 + x + 1$ $CA_{16} = 11001010_2 = x^7 + x^6 + x^3 + x$

Moltiplichiamo come polinomi:

$(x^6 + x^4 + x + 1)(x^7 + x^6 + x^3 + x)$

$= x^{13} + x^{12} + x^9 + x^7$ [da $x^6 \cdot (x^7 + x^6 + x^3 + x)$]

- $x^{11} + x^{10} + x^7 + x^5$ [da $x^4 \cdot (x^7 + x^6 + x^3 + x)$]
- $x^8 + x^7 + x^4 + x^2$ [da $x \cdot (x^7 + x^6 + x^3 + x)$]
- $x^7 + x^6 + x^3 + x$ [da $1 \cdot (x^7 + x^6 + x^3 + x)$]

Combinando (ricordando che in caratteristica 2, a + a = 0):

$= x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + x$

Ora dobbiamo ridurre modulo $m(x) = x^8 + x^4 + x^3 + x + 1$.

Poiché $x^8 \equiv x^4 + x^3 + x + 1 \pmod{m(x)}$, abbiamo: $x^9 \equiv x \cdot x^8 \equiv x^5 + x^4 + x^2 + x$ $x^{10} \equiv x^6 + x^5 + x^3 + x^2$ $x^{11} \equiv x^7 + x^6 + x^4 + x^3$ $x^{12} \equiv x^8 + x^7 + x^5 + x^4 \equiv (x^4 + x^3 + x + 1) + x^7 + x^5 + x^4 \equiv x^7 + x^5 + x^3 + x + 1$ $x^{13} \equiv x^8 + x^6 + x^4 + x^2 + x \equiv x^6 + x^3 + x^2 + 1$

Sostituendo e sommando tutto:

$= (x^6 + x^3 + x^2 + 1) + (x^7 + x^5 + x^3 + x + 1) + (x^7 + x^6 + x^4 + x^3) + (x^6 + x^5 + x^3 + x^2) + (x^5 + x^4 + x^2 + x) + (x^4 + x^3 + x + 1) + x^6 + x^5 + x^4 + x^3 + x^2 + x$

Raggruppando per grado (mod 2):

- x^7: 1 + 1 = 0
- x^6: 1 + 1 + 1 + 1 = 0
- x^5: 1 + 1 + 1 + 1 = 0
- x^4: 1 + 1 + 1 + 1 = 0
- x^3: 1 + 1 + 1 + 1 + 1 + 1 = 0
- x^2: 1 + 1 + 1 + 1 = 0
- x: 1 + 1 + 1 + 1 = 0
- 1: 1 + 1 + 1 = 1

Risultato: $53_{16} \times CA_{16} = 01_{16}$ (sorprendentemente!)

Questo si può verificare notando che CA_{16} è l'inverso moltiplicativo di 53_{16} in $GF(2^8)$.

A.4 Tavola dei Logaritmi Discreti in F_11

Il campo F_11 = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10} ha gruppo moltiplicativo F*_11 di ordine 10.

Verifichiamo che 2 è un generatore (elemento primitivo):

- $2^1 \equiv 2 \pmod{11}$

- $2^2 \equiv 4 \pmod{11}$
- $2^3 \equiv 8 \pmod{11}$
- $2^4 \equiv 16 \equiv 5 \pmod{11}$
- $2^5 \equiv 10 \pmod{11}$
- $2^6 \equiv 20 \equiv 9 \pmod{11}$
- $2^7 \equiv 18 \equiv 7 \pmod{11}$
- $2^8 \equiv 14 \equiv 3 \pmod{11}$
- $2^9 \equiv 6 \pmod{11}$
- $2^{10} \equiv 12 \equiv 1 \pmod{11}$

Quindi 2 genera tutto F*_11. Tavola dei logaritmi in base 2:

Elemento	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
log_2	0	1	8	2	4	9	7	3	6	5

Questa tavola permette di convertire moltiplicazioni in addizioni: log_2(a · b) ≡ log_2(a) + log_2(b) (mod 10)

Esempio: 3 × 5 = 15 ≡ 4 (mod 11) Verifica: log_2(4) = 2, e log_2(3) + log_2(5) = 8 + 4 = 12 ≡ 2 (mod 10) ✓

Appendice B: Tabelle di Riferimento

B.1 Piccoli Gruppi di Galois

Ordine	**Gruppi possibili**	**Esempio di estensione**
1	{e}	K/K (banale)
2	Z/2Z	Q(√2)/Q
3	Z/3Z	Campo di spezzamento di $x^3 - 2$ su Q
4	Z/4Z, Z/2Z × Z/2Z	Q(i, √2)/Q ha gruppo Z/2Z × Z/2Z
5	Z/5Z	Q(ζ_5)/Q
6	Z/6Z, S_3	Campo di spezzamento di $x^3 - 2$ su Q ha gruppo S_3
8	5 gruppi	Q($\sqrt[4]{2}$, i)/Q ha gruppo D_4

B.2 Polinomi Irriducibili su F_2

Grado 2:

- $x^2 + x + 1$

Grado 3:

- $x^3 + x + 1$
- $x^3 + x^2 + 1$

Grado 4:

- $x^4 + x + 1$
- $x^4 + x^3 + 1$
- $x^4 + x^3 + x^2 + x + 1$

Grado 5:

- $x^5 + x^2 + 1$
- $x^5 + x^3 + 1$
- $x^5 + x^3 + x^2 + x + 1$
- $x^5 + x^4 + x^2 + x + 1$
- $x^5 + x^4 + x^3 + x + 1$
- $x^5 + x^4 + x^3 + x^2 + 1$

Grado 8 (usato nell'AES):

- $x^8 + x^4 + x^3 + x + 1$ (polinomio AES)
- $x^8 + x^4 + x^3 + x^2 + 1$
- ... (30 polinomi irriducibili di grado 8 su F_2 in totale)

B.3 Curve Ellittiche Standard per Crittografia

Curve NIST:

1. **P-192:** $y^2 = x^3 - 3x + b$ su F_p con $p = 2^{192} - 2^{64} - 1$
    - Ordine: $\approx 2^{192}$
    - Livello di sicurezza: 96 bit
2. **P-224:** $y^2 = x^3 - 3x + b$ su F_p con $p = 2^{224} - 2^{96} + 1$
    - Ordine: $\approx 2^{224}$
    - Livello di sicurezza: 112 bit
3. **P-256:** $y^2 = x^3 - 3x + b$ su F_p con $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$
    - Ordine: $\approx 2^{256}$
    - Livello di sicurezza: 128 bit

Curve moderne:

4. **Curve25519:** Curva di Montgomery su F_p con $p = 2^{255} - 19$
    - $y^2 = x^3 + 486662x^2 + x$

    - Ottimizzata per efficienza e sicurezza
    - Usata in protocolli moderni (Signal, WhatsApp, TLS 1.3)
5. **Ed25519:** Versione twisted Edwards di Curve25519

    - $-x^2 + y^2 = 1 - (121665/121666)x^2y^2$
    - Usata per firme digitali

B.4 Parametri Crittografici Raccomandati (2024)

Chiavi simmetriche:

- AES-128: 128 bit (sicurezza ≈ 2^{128} operazioni)
- AES-192: 192 bit (sicurezza ≈ 2^{192} operazioni)
- AES-256: 256 bit (sicurezza ≈ 2^{256} operazioni)

Diffie-Hellman su campi finiti:

- Minimo: 2048 bit (sicurezza ≈ 112 bit)
- Raccomandato: 3072 bit (sicurezza ≈ 128 bit)
- Paranoico: 4096 bit (sicurezza ≈ 140 bit)

Curve ellittiche:

- Minimo: 224 bit (sicurezza ≈ 112 bit)
- Raccomandato: 256 bit (sicurezza ≈ 128 bit)
- Paranoico: 384 bit (sicurezza ≈ 192 bit)

Post-quantistico (stime):

- Lattices: Parametri tipici richiedono 1024-2048 elementi
- Codici: Chiavi pubbliche di 100 KB - 1 MB
- Isogenie: 384-512 bit

Bibliografia

Testi Storici Fondamentali

Opere originali di Galois:

- Galois, É. (1846). "Œuvres mathématiques d'Évariste Galois", pubblicato da Joseph Liouville nel Journal de Mathématiques Pures et Appliquées.

Primi sviluppi:

- Jordan, C. (1870). "Traité des substitutions et des équations algébriques".
- Dedekind, R. (1894). "Über die Theorie der ganzen algebraischen Zahlen".

Testi Moderni di Riferimento

Introduttivi:

- Stewart, I. (2015). "Galois Theory" (4th edition). Springer.
- Rotman, J. (1998). "Galois Theory" (2nd edition). Springer.
- Cox, D. A. (2012). "Galois Theory" (2nd edition). Wiley.

Intermedi:

- Garling, D. J. H. (1986). "A Course in Galois Theory". Cambridge University Press.
- Edwards, H. M. (1984). "Galois Theory". Springer.
- Weintraub, S. H. (2008). "Galois Theory" (2nd edition). Springer.

Avanzati:

- Lang, S. (2002). "Algebra" (revised 3rd edition). Springer.
- Jacobson, N. (2009). "Basic Algebra I & II". Dover.
- Morandi, P. (1996). "Field and Galois Theory". Springer.

Teoria dei Numeri e Campi Algebrici

- Neukirch, J. (1999). "Algebraic Number Theory". Springer.
- Marcus, D. A. (1977). "Number Fields". Springer.
- Milne, J. S. (2020). "Algebraic Number Theory".

Applicazioni Crittografiche

Fondamenti:

- Stinson, D. R. & Paterson, M. (2018). "Cryptography: Theory and Practice" (4th edition). CRC Press.
- Hoffstein, J., Pipher, J., & Silverman, J. H. (2014). "An Introduction to Mathematical Cryptography" (2nd edition). Springer.
- Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). "Handbook of Applied Cryptography". CRC Press.

Curve ellittiche:

- Washington, L. C. (2008). "Elliptic Curves: Number Theory and Cryptography" (2nd edition). CRC Press.
- Silverman, J. H. (2009). "The Arithmetic of Elliptic Curves" (2nd edition). Springer.

Post-quantistica:

- Bernstein, D. J., et al. (2009). "Post-Quantum Cryptography". Springer.

Teoria dei Codici

- MacWilliams, F. J. & Sloane, N. J. A. (1977). "The Theory of Error-Correcting Codes". North-Holland.
- Huffman, W. C. & Pless, V. (2003). "Fundamentals of Error-Correcting Codes". Cambridge University Press.
- Lint, J. H. van (1999). "Introduction to Coding Theory" (3rd edition). Springer.

Matematica Computazionale

- Shoup, V. (2009). "A Computational Introduction to Number Theory and Algebra" (2nd edition). Cambridge University Press.
- von zur Gathen, J. & Gerhard, J. (2013). "Modern Computer Algebra" (3rd edition). Cambridge University Press.
- Cohen, H. (1993). "A Course in Computational Algebraic Number Theory". Springer.

Teoria di Galois Avanzata e Generalizzazioni

- Szamuely, T. (2009). "Galois Groups and Fundamental Groups". Cambridge University Press.
- Kharlampovich, O. & Sapir, M. (2011). "Algorithmic Problems in Groups and Semigroups". Birkhäuser.

Riviste e Pubblicazioni Periodiche

- Journal of Algebra - Springer
- Journal of Number Theory - Elsevier
- Journal of Cryptology - Springer
- Designs, Codes and Cryptography - Springer
- Mathematics of Computation - AMS
- Expositiones Mathematicae - Elsevier